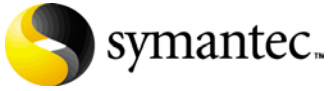
Symantec NetRecon™ 3.6 Security Update 28 Release Notes



Symantec NetRecon Security Update 28 Release Notes

Documentation version: v3.6 060322

Copyright Notice

Trademarks

Technical support

As part of Symantec Security Response, the Symantec Global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site at http://www.symantec.com/techsupp/ for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Platinum support may reach the Platinum Web site at: https://www-secure.symantec.com/platinum/login.html.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC NETRECON SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION. AND/OR ITS SUBSIDIARIES (“LICENSOR”) IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "I DO AGREE" OR “YES” BUTTON OR LOADING THE PRODUCT, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITION, CLICK ON THE "I DO NOT AGREE" OR “NO” BUTTON AND DO NOT USE THE SOFTWARE.

1. License to Use. Licensor grants You a non-exclusive and non-transferable license (the “License”) to use the number of licenses authorized by Your license key of Licensor’s software in machine readable form and accompanying documentation (the “Product”) on Your computer systems or those authorized by Licensor. The License governs any releases, revisions or enhancements to the Product, which Licensor may furnish to You. You may use Product only to scan networks and computer systems for security-related information to detect actual and potential security flaws and vulnerabilities. You may use the Product only to scan or test computer networks, systems or devices owned by You or which You have express permission to access that you have sufficiently backed-up in case of damage caused by this Product. MISUSE OF THE PRODUCT OR DATA GENERATED BY THE PRODUCT IS STRICTLY PROHIBITED BY LICENSOR, MAY VIOLATE U.S. AND OTHER LAWS AND MAY SUBJECT YOU TO SUBSTANTIAL LIABILITY. You are solely responsible for any misuse of the Product Licensed under this Agreement, and You agree to indemnify Licensor for any liability or damage related in any way to Your use of the Product in violation of this Agreement or the rights of any owner or operator of a computer network, system or device. You are also responsible for using the Product in accordance with the limitations of the license You acquired. The types of licenses are as follows: 1) Evaluation License: You may scan an unlimited number of network resources from one system. Each scan is limited to ten minutes unless otherwise authorized by Licensor, and the evaluation license expires in fifteen days unless otherwise authorized by Licensor. 2) Limited License: You may scan Your small network (up to 254 unique network resources) from one system. 3) Unlimited License: You may scan Your large network (an unlimited number of network resources) from one system. 4) Consultant License: You may scan multiple networks belonging to Your customers as long as permission is obtained before such scan, but such scan shall last for no longer than seven days per customer and Product must be removed thereafter. 5) Not For Resell (NFR) License: You may scan multiple networks belonging to Your customers so long as permission is obtained before such scan, but such scan shall last for no longer than fifteen minutes per customer and Product must be removed thereafter. 6) Single Engagement (SE) License: You may scan multiple networks belonging to a single customer for no longer than thirty (30) days. This license is good for use on one of Your customers only and you must obtain permission before any scan is performed. Such scan may only be for delivering assessment services. You will indemnify and hold Licensor harmless for any claims arising out of the use of Product on machines belonging to any of Your customers or any third party that has been provided access to Product or is scanned by You, except to the extent those claims arise out of Licensor's breach of this license.

2. Restrictions. The Product is owned by Licensor, contains valuable trade secrets of Licensor and is protected by copyright, trademark and trade secret laws and international treaties. You agree to use Product only for Your business purposes, and You agree not to provide any other person with a copy of, or access to, any part of Product unless authorized by Your type of license. You may make one copy of Product for back-up, archive or disaster recovery purposes. You may only make copies of documentation as needed for Your internal use of the Product. Each copy of any part of the Product made by or for You must contain all of Licensor’s proprietary markings and copyright notices without alteration. You may not sell, transfer, sublicense, lend, or rent Product to any other person or allow any other person to use Product for any reason, including by making it available for timesharing, service bureau or on-line use. Use by persons to which You have contracted any of Your data processing services is permitted only if each contractor (and its associated employees) is subject to a valid written agreement prohibiting the reproduction or disclosure to other persons of software products and associated Documentation to which they have access and such prohibitions apply to Product. You may not decompile, disassemble, reverse engineer, modify or attempt to discover the source code of Product except as expressly permitted by the laws of the jurisdiction in which You are located, and You may not copy, transfer, or otherwise use Product except as expressly permitted by this license. Use of Product in conjunction with any software product that decompiles or recompiles the Product or in any way creates a derivative or modified copy of Product is an unauthorized use and is prohibited.

3. Limited Warranty. Licensor will replace, at no charge, defective media and product materials that are returned within 30 days of shipment. Licensor warrants, for a period of 30 days the shipment date, that Product will perform in substantial compliance with the written materials accompanying the Product on that hardware and operating system software for which it was designed, as stated in the documentation. Use of Product with hardware and/or operating system software other than that for which it was designed and voids this applicable warranty. If, within 30 days of shipment, You report to Licensor that Product is not performing as described above, and Licensor is unable to correct it within 30 days of the date You report it, You may return Product, and Licensor will refund the License fee. If You promptly notify Licensor of an infringement claim based on an existing U.S. patent, copyright, trademark or trade secret, Licensor will indemnify You and hold You harmless against such claim, and shall control any defense or settlement. This warranty is null and void if You have modified Product, combined the Product with any software or portion thereof owned by any third party that is not specifically authorized or failed promptly to install any version of Product provided to You that is non-infringing. If commercially reasonable, Licensor will either obtain the right for You to use the Product or will modify Product to make it non-infringing. The remedies above are Your exclusive remedies for Licensor's breach of any warranty contained herein.

4. Limitation of Remedies. You understand that the operation of Program may cause problems on or failures of computer networks, systems and devices, which may result in loss of data, unavailability of computing resources or other damage. You represent to Licensor that You own or are authorized to use Product on any computer networks, systems or devices on which Product may be used or that may be tested by Product, You accept all risk of any such damage or loss, any You hereby waive all rights, remedies and causes of action that may arise therefrom. IN NO EVENT WILL LICENSOR OR ITS REPRESENTATIVES BE LIABLE ANY SUCH DAMAGES OR LOSSES WHATSOEVER, INCLUDING ANY LOSS OF PROFITS, LOST SAVINGS, LOSS OF DATA OR LOSS OF USE OR COMPUTER HARDWARE OR SOFTWARE MALFUNCTION OR OTHER SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF LICENSOR OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES. LICENSOR AND ITS REPRESENTATIVES WILL NOT BE LIABLE FOR ANY LOSSES OR DAMAGES CAUSED BY USE OF THE PRODUCT NOT PERMITTED BY THIS AGREEMENT. IN NO EVENT SHALL LICENSOR'S TOTAL LIABILITY UNDER THIS AGREEMENT EXCEED THE AMOUNT PAID FOR THE PRODUCT. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. No action or claim arising out of or relating to this Agreement may be brought by You more than one (1) year after the cause of action is first discovered.

5. Confidentiality. You agree that all information relating to the Product is confidential property of the Licensor ("Proprietary Information"). You will not disclose any Proprietary Information to any third party except to the extent You can document that any such Proprietary Information is in the public domain and generally available for use and disclosure by the general public without any charge or license. If you have obtained a Consultant or NFR license, disclosure to Your clients is permitted only if they have executed a confidentiality agreement that encompasses non-disclosure of Proprietary Information with protections as strict as those contained herein, and such disclosure shall not last longer than allowed by restrictions on use under such license. You recognize and agree that there is no adequate remedy at law for a breach of this section, that such a breach would irreparably harm Licensor and that Licensor is entitled to equitable relief (including, without limitation, injunctive relief) with respect to any such breach or potential breach, in addition to any other remedies available at law.

6. Export Regulation. You agree to comply strictly with all US export control laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses to export, re-export or import the Product. These products are prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria or Sudan.

7. US Government Restricted Rights. If You are acquiring the Product or its accompanying documentation on behalf of the US Government, it is classified as "Commercial Computer Product" and "Commercial Computer Documentation" developed at private expense, contains confidential information and trade secrets of Licensor and its licensors, and is subject to "Restricted Rights" as that term is defined in the Federal Acquisition Regulations ("FARs"). Contractor/Manufacturer is: Symantec Corporation., and its subsidiaries, Cupertino, CA, USA.

8. Miscellaneous. This License is made under the laws of the State of California, USA, excluding the choice of law and conflict of law provisions. This License is the entire License between You and Licensor relating to the Product and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or

additional terms of any quote, order, acknowledgment, or similar communication between the parties during the term of this License. Notwithstanding the foregoing, some Product or products of Licensor may require Licensee to agree to additional terms through Licensor's on-line "click-wrap" license, and such terms shall supplement this Agreement. If any provision of this License is held invalid, all other provisions shall remain valid unless such validity would frustrate the purpose of this License, and this License shall be enforced to the full extent allowable under applicable law. No modification to this License is binding, unless in writing and signed by a duly authorized representative of each party. The License granted hereunder shall terminate upon Your breach of any term herein and you shall cease use of and destroy all copies of Product. Any Product purchased by You after the purchase of the Product which is the subject of this License shall be subject to all of the terms of this License. All of Symantec Corporation’s and its subsidiaries’ licensors are direct and intended third-party beneficiaries of this License and may enforce it against you.

NetRecon Security Update Release Notes

NetRecon Security Update Release Notes

Security Update 28

Symantec NetRecon 3.6 Security Update 28 (SU28) detects and reports 147 new vulnerabilities.

New vulnerability detection

- **Apache MPM Worker.C Denial Of Service Vulnerability**

Apache is prone to a memory leak, causing a denial-of-service vulnerability.

An attacker may consume excessive memory resources, resulting in a denial of service for legitimate users.

Apache 2.x versions are vulnerable; other versions may also be affected.

- **Apache Mod_IMAP Referer Cross-Site Scripting Vulnerability**

Apache's mod_imap module is prone to a cross-site scripting vulnerability. This issue is due to the module's failure to properly sanitize user-supplied input.

An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. This may facilitate the theft of cookie-based authentication credentials as well as other attacks.

- **Apache Mod_SSL Custom Error Document Remote Denial Of Service Vulnerability**

Apache's mod_ssl module is susceptible to a remote denial-of-service vulnerability. A flaw in the module results in a NULL-pointer dereference that causes the server to crash. This issue is present only when virtual hosts are

configured with a custom 'ErrorDocument' statement for '400' errors or 'SSLEngine optional'.

Depending on the configuration of Apache, attackers may crash the entire webserver or individual child processes. Repeated attacks are required to deny service to legitimate users when Apache is configured for multiple child processes to handle connections.

This issue affects Apache 2.x versions.

- **Cisco IOS HTTP Service CDP Status Page HTML Injection Vulnerability**

Cisco IOS HTTP service is reportedly prone to an HTML injection vulnerability.

Specifically the vulnerability affects the Cisco Discovery Protocol (CDP) status page. An attacker can submit malicious HTML and script code through CDP packets to be executed in the context of a logged in administrator. This issue can also allow attackers to execute arbitrary commands on a vulnerable device.

Exploitation can facilitate a variety of attacks such as manipulation of routing information, account creation and access to all other functionality available to administrators.

IOS 11.2(8.11)SA6 is reportedly vulnerable to this issue, however, other versions of IOS 11 are likely affected as well. This issue does not affect IOS 12.

- **Cisco IOS HTTP Service HTML Injection Vulnerability**

Cisco IOS HTTP service is reportedly prone to an HTML injection vulnerability.

An attacker can submit malicious HTML and script code through the '/level/15/exec/-/buffers/assigned' and /level/15/exec/-/buffers/all' scripts. This code may be executed in the browser of an administrator when they attempt to view the contents of memory buffers through the vulnerable scripts of the HTTP service.

This vulnerable has been reported to affect versions of IOS from 11.0 through 12.4. Cisco IOS XR is not vulnerable. As this is a HTML injection vulnerability that targets users of the IOS web interface, devices with the HTTP service disabled are not affected.

Cisco has confirmed this advisory. See Cisco security advisory "cisco-sa-20051201-http" in the reference section.

- **Cisco IOS SGBP Remote Denial of Service Vulnerability**

Cisco IOS SGBP is prone to a remote denial of service vulnerability.

This issue arises on devices that have been configured to run SGBP.

A successful attack causes a device to hang and fail to respond to further requests. It should be noted that a system watchdog timer will detect this condition after a delay and restart the device.

- **Cisco IOS Skinny Call Control Protocol Handler Remote Denial Of Service Vulnerability**

Cisco IOS when configured for Cisco IOS Telephony Service (ITS), Cisco CallManager Express (CME), or Survivable Remote Site Telephony (SRST) services is reported prone to a remote denial of service vulnerability.

The issue is reported to exist in the Skinny Call Control Protocol (SCCP) handler.

A remote attacker may exploit this vulnerability continuously to effectively deny network-based services to legitimate users.

- **Cisco IOS TCLSH AAA Command Authorization Bypass Vulnerability**

Cisco IOS is prone to a remote AAA command authorization-bypass vulnerability. This issue is due to the software's failure to properly enforce command authorization restrictions in the TCL shell.

This issue allows remote attackers to bypass AAA command authorization checks and to gain elevated access to affected devices.

This issue is documented by Cisco bug ID CSCeh73049http://www.cisco.com/pcgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh73049.

- **Cisco Router Online Help Vulnerability**

Under certain revisions of IOS multiple Cisco routers have an information leakage vulnerability in their online help systems. In essence this vulnerability allows users who currently have access to the router at a low level of privilege (users without access to the 'enable' password) can use the help system to view information which should only in theory be available to an 'enabled' user. This information is comprised of access lists among other things. The help system itself does not list these items as being available via the 'show' commands yet none the less it will execute them.

The message which detailed this vulnerability to the Bugtraq mailing list is attached in the 'Credit' section of this vulnerability entry. It is suggested that you read it if this vulnerability affects your infrastructure.

- **GNU SHTool Insecure Temporary File Deletion Vulnerability**

GNU shTool is prone to an insecure temporary file deletion vulnerability.

This issue is due to a design error that causes a file to be insecurely deleted and subsequently and linked file deleted.

An attacker may leverage this issue to delete arbitrary files with the privileges of an unsuspecting user that activates the affected application.

Update (2005/06/11): ocaml-mysql, a package for the Object Camel language that provides access to MySQL, contains shtool code and is vulnerable.

Update (2005/07/14): PHP prior to version 4.4.0 contains shtool code and is vulnerable.

- **MS Visual Studio RAD Support Buffer Overflow Vulnerability**

Due to an unchecked buffer in a subcomponent of FrontPage Server Extensions (Visual InterDev RAD Remote Deployment Support), a specially crafted request via 'fp30reg.dll' could allow a user to execute arbitrary commands in the context of IWAM_machinename on a host running IIS 5.0. A host running IIS 4.0, could allow the execution of arbitrary commands in the SYSTEM context.

- **Microsoft ASN.1 Library Double Free Memory Corruption Vulnerability**

It has been reported that Microsoft ASN.1 library is prone to a double free heap memory corruption vulnerability that may allow a remote attacker to execute arbitrary code on a vulnerable system.

Exploitation of this issue is likely to cause a denial of service condition due to the unique layout of memory structures in affected systems, however, it is possible to leverage this issue via arbitrary code execution to gain system level privileges on a system.

This vulnerability only affects systems that have installed the patch (MS04-007) for BID 9743 (Microsoft ASN.1 Library Multiple Stack-Based Buffer Overflow Vulnerabilities).

- **Microsoft GDI+ Library JPEG Segment Length Integer Underflow Vulnerability**

Microsoft (Graphics Device Interface) GDI+ JPEG handler is reported prone to an integer underflow vulnerability when handling JPEG format images. This issue presents itself due to a lack of sufficient sanity checks performed on certain JPEG data before this data employed as a bounds value for a memory copy operation.

A specially crafted JPEG image may trigger this vulnerability and result in the execution of arbitrary attacker-supplied code. Code execution would occur in the context of the user who is running the vulnerable software.

**Update: This issue is similar in nature to BID 1503, discovered by Solar Designer.

** An exploit that opens a command shell on the local vulnerable system as soon as the image is viewed has been released. Symantec has confirmed that this exploit code is functional. It is important to note that this exploit could potentially be modified to execute other code on the system. Administrators should remain vigilant and patch all vulnerable systems.

- **Microsoft Internet Explorer Cookie Disclosure Vulnerability**

Internet Explorer contains a vulnerability, which could allow an attacker to construct a URL that would allow a malicious website ie information associated with an arbitrary website.

This vulnerability is due to an error parsing hostnames. Specially formatted hostnames can lead to malicious websites being able to read and modify the cookies that other websites have set.

Successful exploitation of this vulnerability could lead to the disclosure of sensitive information such as session IDs, authentication information, etc.

This could assist in further attacks against the user or the webservers that issued the cookies.

- **Microsoft Internet Explorer Cookie Disclosure/Modification Vulnerability**

Internet Explorer contains a vulnerability, which could allow an attacker to construct a URL that would display or modify the cookie information associated with an arbitrary website.

If a URL is composed in the about: protocol referencing a website, Javascript embedded in the URL can access any cookies associated with that website via 'document.cookie'. The Javascript executes because of a cross-site scripting condition in the about: protocol.

- **Microsoft Internet Explorer Patch Q312461 Existence Vulnerability**

The HTTP_USER_AGENT variable gets passed between a web browser and a web server each time a web page is requested by a program. The variable contains the user agent name along with operating system information.

An issue exists with Microsoft Internet Explorer patch Q312461 which, when installed, will reveal its existence in the HTTP_USER_AGENT variable.

This issue could assist an attacker in locating unpatched browsers and launching attacks against the target.

- **Microsoft NNTP Component Heap Overflow Vulnerability**

The Microsoft Network News Transfer Protocol (NNTP) Component is prone to a buffer overflow condition. Successful exploitation of this vulnerability could allow remote code execution in the context of the process accessing the vulnerable component.

- **Microsoft Negotiate SSP Remote Buffer Overflow Vulnerability**

The Microsoft Negotiate Security Software Provider (SSP) interface is prone to a remote buffer overflow vulnerability. In most cases, exploitation would result in a denial of service, but arbitrary code execution is possible.

- **Microsoft Network Monitor Multiple Buffer Overflow Vulnerabilities**

The Network Monitor tool that ships with Windows NT/2000 allows and administrator to capture and analyze all network traffic on the local network as well as traffic destined for the host. Netmon is designed to capture this traffic before being viewed in the graphical interface by parsing information received from the network and then translated into a readable format in the user interface.

Seperate DLL libraries within Netmon parse the individual application protocols. One of these libraries, "browser.dll" is vulnerable. By exploiting multiple stack overflows in various function calls within the vulnerable dll's, a remote attacker could gain control of Network Monitor and execute arbitraty code and gaining control of the victim host.

- **Microsoft PhoneBook Server Buffer Overflow**

The Phone Book Service is an optional component that ships with the NT 4 Option Pack and Windows 2000. It is not installed by default.

A buffer overflow vulnerability was discovered in the URL processing routines of the Phone Book Service requests on IIS 4 and IIS 5. If exploited, this vulnerability allows an attacker to execute arbitrary code and obtain a remote command shell with those privileges of the IUSR_machinename account (IIS 4) or the IWAM_machinename account (IIS 5).

- **Microsoft Temporary Internet File Execution Vulnerability**

Temporary Internet Files (TIFs) are formatted files used to store content cached from Internet communications. TIFs are created by a number of Microsoft applications, such as Outlook, Outlook Express, and Internet Explorer.

Under some circumstances, it may be possible to execute files within a TIF. When an application such as Internet Explorer 6.0 or Outlook 2002 receives files from outside, the files are transferred to a TIF using a .TMP extension. Through the use of MIME base64, it is possible to place a set of files on a system that, when decoded and stored in a directory, may be sequentially and arbitrarily executed.

- **Microsoft UPnP NOTIFY Buffer Overflow Vulnerability**

Universal Plug and Play, or UPnP, is a service that allows for hosts to locate and use devices on the local network. UPnP support ships with Windows XP and ME. For Windows 98 and 98SE, it is available with Windows XP's Internet Connection Sharing client. It should be noted that UPnP services are enabled on Windows XP by default.

When processing the location field in a NOTIFY directive, UPnP server process memory can be overwritten by data that originated in the packet. If the IP address, port and filename components are of excessive length, access

violations will occur when the server attempts to dereference pointers overwritten with data from the packet.

It should be noted that the service listens on broadcast and multicast interfaces. This could permit an attacker to exploit a number of systems without knowing their individual IP addresses, if they employed an exploitation method targeting a UDP port. It is however possible to exploit this condition using either the TCP or UDP protocols.

The UPnP service runs in the LOCAL SERVICE security context. An attacker who successfully exploits this vulnerability could gain control over the target host.

- **Microsoft Universal Plug and Play Simple Service Discovery Protocol Denial of Service Vulnerability**

Universal Plug and Play, or UPnP, is a service that allows for hosts to locate and use devices on the local network. UPnP support ships with Windows XP and ME. For Windows 98 and 98SE, it is available with Windows XP's Internet Connection Sharing client.

The Simple Service Discovery Protocol (SSDP) is a component of UPnP that allows a system to enumerate the resources of a newly installed network device on a UPnP network. This service is vulnerable to a denial of service condition by constructing a UDP packet directed at a UPnP-enabled system which directs the system to an echoed port, the system would enter into an endless download cycle.

This vulnerability could possibly be used to launch a distributed denial of service attack by directing several UPnP-enabled systems at a third party.

- **Microsoft Virtual DOS Machine Local Privilege Escalation Vulnerability**

A problem exists in the Virtual DOS Machine (VDM) that may allow a local user to elevate their privilege level. The issue exists because an attacker may use the VDM to write arbitrary code to protected kernel memory locations.

- **Microsoft Windows 2000 Domain Controller LDAP Denial Of Service Vulnerability**

A denial of service vulnerability has been reported in Microsoft Windows 2000 Server systems that are acting as Domain Controllers.

This issue may be triggered by sending a malformed LDAP query to an affected Windows 2000 Domain Controller. This will cause a reboot in the Domain Controller and may be exploited repeatedly to cause a persistent denial of service.

Microsoft Windows Embedded Web Font Buffer Overflow Vulnerability

Microsoft Windows is susceptible to a remotely exploitable buffer-overflow vulnerability. This issue is due to the software's failure to properly bounds-check user-supplied input before copying it to an insufficiently sized memory buffer.

This issue allows remote attackers to execute arbitrary machine code in the context of the vulnerable software on the targeted user's computer.

- **Microsoft Windows Graphics Rendering Engine WMF SetAbortProc Code Execution Vulnerability**

Microsoft Windows WMF graphics rendering engine is affected by a remote code-execution vulnerability. This issue affects the 'SetAbortProc' function.

The problem presents itself when a user views a malicious WMF formatted file, triggering the vulnerability when the engine attempts to parse the file.

The issue may be exploited remotely or locally. Any remote code execution that occurs will be with the privileges of the user viewing a malicious image. An attacker may gain SYSTEM privileges if an administrator views the malicious file.

Local code execution may facilitate a complete compromise.

- **Microsoft Windows H.323 Remote Buffer Overflow Vulnerability**

The Microsoft Windows H.323 protocol implementation is prone to a remote buffer overflow. Successful exploitation could allow for execution of arbitrary code.

This vulnerability could only be exploited if an H.323 application such as NetMeeting were running on the system.

- **Microsoft Windows Help Facilities Vulnerabilities**

Microsoft has reported two vulnerabilities in its Windows Help Facilities.

The first vulnerability is in a function exposed in an ActiveX control. Attackers may invoke and exploit the control through a malicious webpage or HTML email. The vulnerability is a buffer overflow condition and may be levaraged by attackers to execute arbitrary code on victim systems. Any code executed would run in the security context of Explorer.

The second vulnerability involves Compiled Help Files (chm) and may allow for attackers to execute commands on the victim host. The Help Facilities component will execute potentially malicious .chm files in the Temporary Internet Files folder. This behaviour has been corrected in a patch developed by Microsoft.

**Note: This database entry is temporary. New vulnerabilities are to be given unique Bugtraq IDs and alerts will be published for each individual issue. This BID will be retired when analysis is complete.

- **Microsoft Windows Help Facility ActiveX Control Buffer Overflow Vulnerability**

The ActiveX control that provides much of the functionality for the Windows Help Center contains an unchecked buffer. Successful exploitation could result in execution of arbitrary code in the security context of the current user.

- **Microsoft Windows IGMPv3 Denial of Service Vulnerability**

A vulnerability in the handling of IGMPv3 (Internet Group Management Protocol) packets could result in a denial of service.

An attacker can exploit this issue through a broadcast attack to cause vulnerable computers on the subnet to become unresponsive, effectively denying service to legitimate users.

- **Microsoft Windows License Logging Service Buffer Overflow Vulnerability**

A buffer overflow exists in the Microsoft Windows License Logging Service. This could allow remote execution of arbitrary code.

- **Microsoft Windows Local Descriptor Table Local Privilege Escalation Vulnerability**

Microsoft Windows Local Descriptor Table programming interface has been reported prone to a privilege escalation vulnerability

As a result of this it is reportedly possible for a local attacker to create a malicious entry into the Local Descriptor Table. This entry may point into protected memory. Because this memory space is reserved for kernel operations, it is likely that an attacker will exploit this condition to execute arbitrary code with elevated privileges.

- **Microsoft Windows Multiple Local Privilege Escalation Vulnerabilities**
- **Microsoft Windows Private Communications Transport Protocol Buffer Overrun Vulnerability**

Various Microsoft Windows operating systems are prone to a remotely exploitable stack-based buffer overrun via the PCT (Private Communications Transport) protocol. Successful exploitation of this issue could allow a remote attacker to execute malicious code on a vulnerable system, resulting in full system compromise.

The vulnerability may also reportedly be exploitable by a local user who passes malicious parameters to the vulnerable component interactively or through another application.

This issue is reported to only affect systems that have SSL enabled, such as web servers, but could also affect Windows 2000 Domain Controllers under some circumstances. For Windows Server 2003, PCT must be manually enabled in

addition to enabling SSL support to be affected. Reportedly, both PCT 1.0 and SSL 2.0 must be enabled for successful exploitation.

The DeepSight Threat Analysis team has observed exploit activity in the wild associated with this vulnerability.

- **Microsoft Windows SSL Library Denial of Service Vulnerability**

Microsoft Windows SSL library is reported to be prone to a denial of service vulnerability. It has been reported that an attacker could trigger this issue by sending a specially crafted TCP message that causes the protocol to fail resulting in a denial of service.

Successful exploitation of this issue in Windows 2000 and Windows XP would cause the systems to stop accepting SSL connections. The issue leads to a system restart in Windows Server 2003.

- **Microsoft Windows Server Message Block Handlers Remote Buffer Overflow Vulnerability**

Microsoft Windows Server Message Block handler is reported prone to a remote buffer overflow vulnerability.

It should be noted that SMB drivers execute in the kernel memory space and a successful attack can allow a remote attacker to gain unauthorized access with ring 0 privileges.

Microsoft has noted that other protocols, such as IPX/SPX, could also be vulnerable to this issue.

**Update: It is reported that Microsoft Windows NT 4.0 has also been found vulnerable to the issue that is described in this BID.

- **Microsoft Windows Trusted Domain Privilege Escalation Vulnerability**

Trust relationships can be configured between domains controlled by Microsoft Windows 2000 and NT Server. These trust relationships allow for 'trusted domains' to access resources on 'trusting domains'.

Windows 2000 and NT contain a vulnerability in this feature that may allow for an attacker with administrative privileges on a trusted domain to elevate privileges on any trusting domain.

It is possible for a trusted domain to associate any SID (security identifier) with any security group in the trusting domain. A malicious administrator or an attacker who has obtained administrative privileges on a trusted domain may exploit this vulnerability to obtain control of the trusting domain. For example, a trusted domain may associate a local (within the trusted domain) user SID with the administrative security group on the trusting domain. The SID would then have the privileges of the administrative group within the trusting domain.

It should be noted that it is difficult to exploit this vulnerability.

Microsoft Windows 2000 and NT provide no facility or API allowing for modification of the authorization data required to exploit this vulnerability.

- **Microsoft Windows Utility Manager Local Privilege Escalation Vulnerability**

Microsoft Utility Manager has been reported prone to a local privilege escalation vulnerability. It is reported that a local user may influence the Utility Manager into executing arbitrary code.

A local attacker may exploit this vulnerability to have arbitrary attacker-supplied code executed with SYSTEM privileges.

- **Microsoft Windows WINS Association Context Data Remote Memory Corruption Vulnerability**

It is reported that the WINS replication protocol contains a vulnerability that when exploited will result in memory corruption. The issue exists due to a protocol design flaw that allows a remote user to specify the location of an association context data structure in memory.

Because the attacker may control the location of the data structure, this vulnerability may be exploited to corrupt process memory.

This issue could potentially be exploited remotely by a WINS client to execute arbitrary code with SYSTEM level privileges on a target WINS server. The service may be exposed via TCP/UDP port 42 by default, but the vendor has stated that other attack vectors may exist though none are known at this time.

The WINS service is not installed by default on most Microsoft Windows platforms.

** UPDATE: The WINS service is installed and enabled by default on Microsoft Small Business Server 2000/2003. However, the ports used for the service are reportedly not remotely accessible by default on Small Business Server.

- **Microsoft Windows WINS Name Value Handling Remote Buffer Overflow Vulnerability**

It is reported that the WINS server contains a buffer overflow vulnerability that when exploited will result in WINS process memory corruption. The issue exists due to a lack of sufficient boundary checks performed on computer 'name' data that is handled during a WINS transaction.

Ultimately, the issue could potentially be exploited remotely by a WINS client to execute arbitrary code with SYSTEM level privileges on a target WINS server. The service may be exposed via TCP/UDP port 42 by default, but the vendor has stated that other attack vectors may exist though none are known at this time.

- **Microsoft Windows WMF/EMF Image Formats Remote Buffer Overflow Vulnerability**

It has been reported that Windows may be prone to a remote buffer overflow vulnerability when rendering WMF/EMF image files. An attacker could create a malicious WMF or EMF file and entice a user to view the file via an application that supports the WMF and EMF formats. Immediate consequences of this attack may result in a denial of service condition, however, it is possible that an attacker could leverage this issue to execute arbitrary code in the context of the vulnerable user.

This issue may be similar to the vulnerabilities described in BID 9892 (Microsoft Windows XP explorer.exe Remote Denial of Service Vulnerability) and BID 9707 (Microsoft Windows XP explorer.exe Multiple Memory Corruption Vulnerabilities).

- **Microsoft Windows Web Client Buffer Overflow Vulnerability**

Microsoft Windows Web Client is prone to a buffer overflow. Successful exploitation could allow arbitrary code execution with System privileges.

- **Multiple Vendor TCP/IP Resource Exhaustion Vulnerability**

Microsoft's implementation NetBIOS is vulnerable to a remotely exploitable denial of service attack. An attacker who has access to the NBT port can cause the system to become exhausted of network resources and cease functioning.

The attack is carried out by initiating many connections and then closing them, leaving the target tcp sockets in FINWAIT_1 state. Although the sockets will eventually time out and be freed, an attacker can continuously send more, initiating and closing new connections using up any freed network resources. The result may be a denial of useful NetBIOS services until the attack stops.

This type of attack is well known as simple resource exhaustion, but has become an issue with new tools that enable attackers to launch more effective resource exhaustion attacks. Microsoft has released fixes to patch this vulnerability in NT 4.0sp6. This vulnerability affects many operating systems aside from Microsoft Windows, however Microsoft is the only vendor thus far to issue a patch and workaround.

- **MySQL AB MySQL Multiple Remote Vulnerabilities**

MySQL is reported prone to multiple vulnerabilities that can be exploited by a remote authenticated attacker. The following individual issues are reported:

- Insecure temporary file-creation vulnerability. Reports indicate that an attacker with 'CREATE TEMPORARY TABLE' privileges on an affected installation may leverage this vulnerability to corrupt files with the privileges of the MySQL process.

- Input-validation vulnerability. Remote attackers with INSERT and DELETE privileges on the 'mysql' administrative database can exploit this. Reports indicate that this issue may be leveraged to load and execute a malicious library in the context of the MySQL process.
- Remote arbitrary-code execution vulnerability. Reportedly, the vulnerability may be triggered by employing the 'CREATE FUNCTION' statement to manipulate functions to control sensitive data structures. This issue may be exploited to execute arbitrary code in the context of the database process.

These issues are reported to exist in MySQL versions prior to MySQL 4.0.24 and 4.1.10a.

- **MySQL Aborted Bug Report Insecure Temporary File Creation Vulnerability**

The MySQL bug reporting utility (mysqlbug) creates a temporary file with a static name when a bug report is aborted. An attacker may exploit this issue to launch symbolic link attacks that will most likely result in corruption of files. This could cause destruction of data and denial of services.

This issue would only affect Unix/Linux-based operating systems.

- **MySQL Authentication Bypass Vulnerability**

MySQL is prone to a vulnerability that may permit remote clients to bypass authentication.

This is due to a logic error in the server when handling client-supplied length values for password strings.

Successful exploitation will yield unauthorized access to the database.

This issue is known to exist in MySQL 4.1 releases prior to 4.1.3 and MySQL 5.0.

- **MySQL Bounded Parameter Statement Execution Remote Buffer Overflow Vulnerability**

It is reported that MySQL is susceptible to a buffer overflow vulnerability. This issue is due to a failure of the application to properly ensure the size of a buffer is sufficient to handle user-supplied input data before performing operations that may overflow into adjacent memory regions.

This vulnerability reportedly allows for remote attackers to crash affected servers. It is unconfirmed, but there may be a possibility of remote code execution in the context of the affected server. It would likely require a complex exploit, in order to take advantage of overwriting memory contents with NULL bytes. Attackers may be able to take advantage of the structured, predictable nature of the memory operations in order to control the flow of execution of the application.

MySQL versions 4.1.3-beta and 4.1.4 are reported vulnerable, but other versions are also likely affected.

- **MySQL Database MySQLAccess Local Insecure Temporary File Creation Vulnerability**

A local insecure temporary file creation vulnerability affects the MySQL Database. This issue is due to a failure of a script bundled with the application to securely create temporary files in globally accessible locations.

An attacker may leverage this issue to corrupt arbitrary files with the privileges of the user that activates the vulnerable script.

- **MySQL Database Unauthorized GRANT Privilege Vulnerability**

It is reported that MySQL is susceptible to an unauthorized database GRANT privilege vulnerability. This issue is due to a failure of the application to ensure that users have sufficient privileges to issue the GRANT command.

By exploiting this vulnerability, attackers may reportedly be able to gain unauthorized access to databases. This may allow them to read or modify the contents of potentially sensitive databases located on the same database server.

Versions of MySQL prior to 4.0.21 are reported vulnerable to this issue.

- **MySQL MYSQLD_Multi Insecure Temporary File Creation Vulnerability**

Mysqld_multi is reported prone to insecure temporary file handling. The script likely creates temporary files with predictable filenames.

An attacker may exploit this issue to launch symbolic link attacks that will most likely result in corruption of files when the vulnerable script is launched.

This issue would only affect Unix/Linux-based operating systems.

- **MySQL Multiple Local Vulnerabilities**

MySQL is reported prone to multiple local vulnerabilities. These issues may allow an attacker to bypass security restrictions or cause a denial of service condition in the application.

It is reported that an attacker can bypass certain security restrictions and gain access to and corrupt potentially sensitive data due to an error in 'ALTER TABLE ... RENAME' operations.

A denial of service condition presents itself when multiple threads ALTER MERGE tables to change the UNION.

Due to a lack of details, further information is not available at the moment. This BID will be updated as more information becomes available.

- **MySQL Mysqlhotcopy Script Insecure Temporary File Creation Vulnerability**

Mysqlhotcopy is reported to contain an insecure temporary file creation vulnerability. The result of this is that temporary files created by the application may use predictable filenames. This issue presents itself when the 'scp' method is used with the script.

A local attacker may also possibly exploit this vulnerability to execute symbolic link file overwrite attacks.

It was confirmed that this issue exists in mysqlhotcopy shipped with MySQL 3.23.49 and 4.0.20. Other versions of MySQL are likely to be affected as well. This BID will be updated as more information becomes available.

- **MySQL Password Length Remote Buffer Overflow Vulnerability**

MySQL is prone to a remotely exploitable stack-based buffer overflow vulnerability.

This issue exists in the password checking routines and may be triggered by a malicious authentication packet.

Exploitation will be complicated by the fact that the exploit string will be scrambled with a random number generator and may also require a valid password hash. However, if successfully exploited, the attacker may execute arbitrary code in the context of the server.

This issue is known to exist in MySQL 4.1 releases prior to 4.1.3 and MySQL 5.0.

- **MySQL Query Logging Bypass Vulnerability**

MySQL is susceptible to a query-logging-bypass vulnerability. This issue is due to a discrepency between the handling of NULL bytes in input data.

This issue allows attackers to bypass the query-logging functionality of the database so they can cause malicious SQL queries to be improperly logged. This may help them hide the traces of malicious activity from administrators.

This issue affects MySQL version 5.0.18; other versions may also be affected.

- **MySQL Remote FULLTEXT Search Denial Of Service Vulnerability**

MySQL is affected by a remote denial of service vulnerability in its FULLTEXT search functionality. This issue is due to a failure of the application to handle exceptional search input.

An attacker can leverage this issue to cause the affected MySQL database to crash, denying service to legitimate users.

- **MySQL Unspecified Insecure Temporary File Creation Vulnerability**

MySQL is affected by an unspecified insecure temporary file creation vulnerability. This issue is likely due to a design error that causes the application to fail to verify the existance of a file before writing to it.

An attacker may leverage this issue to overwrite arbitrary files with the privileges of an unsuspecting user that activates the vulnerable application. Reportedly this issue is unlikely to facilitate privilege escalation.

- **MySQL User-Defined Function Buffer Overflow Vulnerability**

MySQL is prone to a buffer overflow vulnerability. This issue is due to insufficient bounds checking of data supplied as an argument in a user-defined function.

This issue could be exploited by a database user with sufficient access to create a user-defined function. It may also be possible to exploit this issue trhough latent SQL injection vulnerabilities in third-party applications that use the database as a backend.

Successful exploitation will result in execution of arbitrary code in the context of the database server process.

- **MySQL mysql_install_db Insecure Temporary File Creation Vulnerability**

MySQL is reportedly affected by a vulnerability that can allow local attackers to gain unauthorized access to the database or gain elevated privileges. This issue results from a design error due to the creation of temporary files in an insecure manner.

The vulnerability affects the 'mysql_install_db' script.

Due to the nature of the script, an attacker may create database accounts or gain elevated privileges.

MySQL versions prior to 4.0.12 and MySQL 5.x releases 5.0.4 and prior are reported to be affected.

- **Oracle /tmp Race Condition Vulnerability**

The Oracle binary, 'oracle', for Unix systems is believed to contain a race condition vulnerability.

The vulnerability is related to the use of temporary files in a user-definable directory. The filename is predictable.

Attackers can exploit this vulnerability to corrupt files writeable by user 'oracle' via a symbolic link attack.

- **Oracle 8 File Access Vulnerabilities**

A number of security file access security vulnerabilities in suid programs that are part of Oracle may be exploited to obtain the privileges of the 'oracle' user

and full access to the database system. Only the Unix version of Oracle is vulnerable.

The following suid executables are believed to contain security vulnerabilities: lsnrctl, oemevent, onrsd, osslogin, tnslsnr, tnsping, trcasst, trcroute, cmctl, cmadmin, cmgw, names, namesctl, otrccref, otrcfmt, otrcrep, otrccol and oracleO. These files are owned by the oracle user and are suid.

The utilities implement insecure file creation and manipulation and they trust environment variables. These allow malicious users to create, append or overwrite files owned by the oracle user, as well as executing program as the oracle user.

- **Oracle 8 oratclsh Suid Vulnerability**

Oracle8 is an enterprise level database. As part of the Internet Agent option installation process it installs the file $ORACLE_HOME/bin/oratclsh as suid root. oratclsh is a TCL application that provides full access to TCL. oratclsh gives anyone the ability to execute arbitrary TCL commands as root.

The suid root bit gets set when the post install script "root.sh" is executed as root as directed in the installation instructions. If the "root.sh" script is not executed as root after installing the Intelligent Agent the oratclsh will be owned by the installation user (typically oracle). Although not as degerous as suid root, a suid oracle oratclsh script would allow a malicious user to obtain full acess to the database.

The offending core in "root.sh":

Setuid to root for oemagent executables

/bin/chown root /oracle/bin/dbsnmp

/bin/chmod u+s /oracle/bin/dbsnmp

/bin/chown root /oracle/bin/oratclsh

/bin/chmod u+s /oracle/bin/oratclsh

- **Oracle 8i Listener Remote Redirect Denial of Service Vulnerability**

A denial of service vulnerability exists in Oracle 8i servers running on Windows NT. Repeated requests to an Oracle listener, which redirects connections to a seperate port, could cause the host to stop responding.

- **Oracle 8i TNS Listener Buffer Overflow Vulnerability**

Oracle 8i ships with a component called TNS Listener. TNS Listener is used to arbitrate communication between remote database clients/applications and the database server.

There exists a remotely exploitable buffer overflow in TNS Listener. Remote attackers can execute arbitrary code on affected hosts. This vulnerability does not require authentication to exploit.

On Windows 2000/NT4 systems, TNS Listener runs with 'LocalSystem' privileges. These are equivelent to administrative and any attacker to exploit this vulnerability on such a system would gain control over it.

On Unix systems, Oracle processes such as the listener typically run as their own userid. Exploitation of this vulnerability on these systems would provide an attacker with local access to the victim host. It is significantly easier for attackers to compromise the entire system with local access.

Note: Versions 8.1.5, 8.1.6, and 8.1.7 are confirmed as being vulnerable. Previous versions are likely vulnerable as well.

- **Oracle 8i TNS Listener Local Command Parameter Buffer Overflow Vulnerability**

Oracle 8i is a powerful relational database product. It is available for Windows, Linux, and a wide range of Unix operating systems.

A vulnerability has been reported with some versions of Oracle 8i for Linux. A local attacker able to execute the tnslsnr process may pass an oversized command line parameter and cause a buffer overflow, possibly leading to the execution of arbitrary code as the user 'oracle'.

Versions of Oracle 8i available for other operating systems have not yet been confirmed as vulnerable.

- **Oracle 8i dbsnmp Command Remote Denial of Service Vulnerability**

Oracle 8i is an enterprise level database solution. It is available on a wide variety of platforms, including many Unix operating systems.

It is possible to cause a denial of service condition in Oracle 8i. If either of the dbsnmp_start or dbsnmp_stop commands are sent remotely to the TNS listener service, a memory error will occur. The Oracle documentation states that these commands should only be used locally.

- **Oracle 9i Default Configuration File Information Disclosure Vulnerability**

Oracle 9iAS includes two important configuration files called "XSQLConfig.xml" and "soapConfig.xml". The configuration files contain sensitive information, such as database usernames and passwords.

Both of these files are accessible to remote clients without any authentication. It is possible for malicious users to access and read the files through a virtual directory.

Possibly sensitive information disclosed to attackers may assist in further attacks.

- **Oracle 9iAS Apache PL/SQL Module Denial of Service Vulnerability**

The Oracle 9iAS web service is powered by the Apache webserver. Included is an Apache module for PL/SQL support.

If a request is made to the pls module with a HTTP client authorization header set, and with no auth type defined, the server will suffer an access violation error. A restart is required in order to regain normal functionality.

It has been reported that this is not the result of a buffer overflow, and it is not believed to be exploitable to execute code.

- **Oracle 9iAS Apache PL/SQL Module Multiple Buffer Overflows Vulnerability**

The Oracle 9iAS web service is powered by the Apache webserver. Included is an Apache module for PL/SQL support.

The Oracle 9iAS PL/SQL module is vulnerable to several buffer overflow conditions. Exploitation of these conditions may allow for attackers to execute arbitrary code remotely.

On Windows based systems, the module is run within the local SYSTEM security context. On Unix systems, the webserver may run with user-level privileges.

- **Oracle 9iAS Apache PL/SQL Module Web Administration Access Vulnerability**

The Oracle 9iAS web service is powered by the Apache webserver. Included is an Apache module for PL/SQL support. Administrative web pages associated with this server allow a web user to modify Database Access Descriptors and cache settings.

By default, no authentication is required to access these administrative pages. As a result, any attacker able to access the page may perform these administrative functions. The ability to modify DAD settings may allow an attacker to access or modify PL/SQL applications, or deny service to legitimate users.

- **Oracle Database 8i/9i Multiple Remote Directory Traversal Vulnerabilities**

Oracle Database server is reported prone to multiple directory traversal vulnerabilities that may allow a remote attacker to read, write, or rename arbitrary files with the privileges of the Oracle Database server.

The issues are reported to exist due to a lack of sufficient input validation performed on filenames and paths passed to file processing functions, and may

allow a malicious SQL query to traverse outside of a directory that is described in an Oracle directory object.

- **Oracle Database Auditing Insecure Default Configuration Vulnerability**

Oracle is a commercial relational database product. Oracle is available for the Unix, Linux, and Microsoft Windows platforms.

An insecurity exists in the default configuration of Oracle database. Oracle Auditing is disabled in the default install and must be enabled by the user of the products. Oracle Auditing provides an interface for accounting of specific database objects, operations, users, and privileges.

As a result malicious activity may go undetected.

- **Oracle Database Default Library Directory Privilege Escalation Vulnerability**

Oracle database implementations are reportedly prone to a default library directory privilege escalation vulnerability. This issue arises due to a default configuration error that will permit the attacker to replace libraries required by setuid root applications with arbitrary code.

This issue would allow an Oracle software owner to execute code as the superuser, taking control of the entire system.

It should be noted that this vulnerability only affects Oracle on UNIX/Linux platforms.

- **Oracle Database Multiple SQL Injection Vulnerabilities**

Oracle database is reported prone to multiple SQL injection vulnerabilities. These issues exist due to insufficient sanitization of user-supplied data.

These issues can be exploited using malformed PL/SQL statements to pass unauthorized SQL statements to the database. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation.

Some of these issues may have been reported in BID 13139 (Oracle Multiple Vulnerabilities) and addressed by the Oracle Critical Patch Update - April 2005. This cannot be confirmed at the moment.

This BID will be updated and divided into individuals BIDs as more information becomes available.

- **Oracle Database Multiple Vulnerabilities**

Oracle Database 10g, Oracle9i Database Server, Oracle8i Database Server, Oracle8 Database, Oracle Collaboration Suite, Oracle Application Server, and Oracle E-Business Suite are reported prone to multiple vulnerabilities.

Oracle has released a Critical Patch Update to address these issues in various supported applications. The following specific issues were identified:

- A networking component of Oracle8 Database is affected by a vulnerability.
- The LOB Access component of Oracle8i Database Server is reported prone to an information disclosure vulnerability.
- The Spatial component of Oracle8i Database Server is reported prone to a vulnerability.
- The UTL_FILE component of Oracle9i Database Server Release 2 is reported prone to a vulnerability.
- A Diagnostic component of Oracle8i Database Server is reported prone to a vulnerability.
- The XDB component of Oracle Database 10g and Oracle9i Database Server Release 2 is reported prone to multiple vulnerabilities.
- The Dataguard component of Oracle Database 10g is reported prone to a vulnerability.
- The Log Miner component of Oracle9i Database Server Release 2 is reported prone to a vulnerability.
- The OLAP component of Oracle9i Database Server Release 2 is reported prone to a vulnerability.
- The Data Mining component of Oracle Database 10g is reported prone to a vulnerability.
- The Advanced Queuing component of Oracle Database 10g is reported prone to a vulnerability.
- The Change Data Capture component of Oracle Database 10g is reported prone to multiple vulnerabilities.
- The Database Core component of Oracle Database 10g is reported prone to a vulnerability.
- The OHS component of Oracle Database 10g is reported prone to a vulnerability.
- The Report Server component of Oracle Application Server is reported prone to a vulnerability.
- The Forms component of Oracle Application Server is reported prone to a vulnerability.
- The mod_plsql component of Oracle Application Server is reported prone to a vulnerability.

- The Calendar component of Oracle Collaboration Suite is reported prone to a vulnerability.
- The Oracle E-Business Suite is reported prone to multiple vulnerabilities.

The Oracle advisory only addresses those products that are supported. It is likely that earlier versions of the releases may also be affected. This Critical Patch Update also includes Oracle Security Alert #68 fixes that are specified in BID 10871 (Oracle Multiple Unspecified Vulnerabilities), BID 11120 (Oracle Database 9i SQL Command Buffer Overflow Vulnerability), BID 11099 (Oracle Database Server ctxsys.driload Access Validation Vulnerability), BID 11100 (Oracle Database Server dbms_system.ksdwrt Remote Buffer Overflow Vulnerability), and BID 11091 (Oracle 10g Database DBMS_SCHEDULER Remote Command Execution Vulnerability).

It is possible that other BIDs such as BID 12296 (Oracle Database Multiple Unspecified Vulnerabilities) are related to these vulnerabilities as well.

This BID will be divided and updated into separate BIDs when more information is available.

- **Oracle Database Server DIRECTORY Buffer Overflow Vulnerability**

Oracle has announced a vulnerability in the Oracle 9i Database Server. This issue affects Oracle 9i Release 2 and earlier.

It has been reported that a buffer overflow condition may occur in the BFILENAME function when run with malicious arguments. This issue likely occurs due to insufficient bounds checking on user-supplied input.

As this issue allows a user to overwrite memory, it may be possible for an attacker to exploit this vulnerability to execute commands.

- **Oracle Database Server EXTPROC Buffer Overflow Vulnerability**

The EXTPROC executable used by the Oracle Database Server is prone to a buffer overflow. Successful exploitation could result in arbitrary code execution with potentially elevated privileges.

** This issue is reportedly related to BID 4033. A reliable source has indicated that Oracle patches for the issue described in BID 4033 introduce this issue. Symantec has not been able to confirm this information.

- **Oracle Database Server TO_TIMESTAMP_TZ Buffer Overflow Vulnerability**

Oracle Database Server is prone to a buffer overflow in the TO_TIMESTAMP_TZ function. Malicious users who can execute this function with malformed parameters or influence a query which causes this function to be executed may exploit this vulnerability. Successful exploitation will enable the attacker to execute malicious instructions in the context of the database server.

- **Oracle Database Server TZ_OFFSET Buffer Overflow Vulnerability**

Oracle Database Server contains an unchecked buffer in the TZ_OFFSET function. Malicious users who can execute this function with malformed parameters or influence a query which causes this function to be executed may exploit this vulnerability. Successful exploitation will enable the attacker to execute malicious instructions in the context of the database server.

- **Oracle Database Server ctxsys.driload Access Validation Vulnerability**

Oracle Database Server is prone to an access validation vulnerability that may permit unprivileged users to execute commands as the DBA. This could compromise the database.

This issue corresponds to one of the unspecified vulnerabilities mentioned in BID 10871 and addressed by Oracle Alert #68.

- **Oracle Database Server dbms_system.ksdwrt Remote Buffer Overflow Vulnerability**

A remotely exploitable buffer overflow exists in Oracle Database Server.

The issue can be triggered when an overly long string is passed to an internal logging function. Authorized users could exploit this issue to execute arbitrary code in the context of the server process or to cause a denial of service.

This issue corresponds to one of the unspecified vulnerabilities mentioned in BID 10871 and addressed by Oracle Alert #68.

- **Oracle Database Windows XP Simple File Sharing Authentication Bypass Vulnerability**

Oracle Database is affected by an authentication bypass vulnerability when run on Microsoft Windows XP computers that have Simple File Sharing enabled.

This vulnerability may let attackers compromise the database using the Windows XP Guest account.

The researcher who discovered this issue has not provided a conclusive list of affected Oracle database products. For the time being, all versions that run on Windows XP are assumed to be affected. If contrary information is made available, this BID will be updated accordingly.

- **Oracle Internet Directory 2.0.6 oidldap Vulnerability**

Oracle Internet Directory 2.0.6 is a pre-alpha development release, available as both an addon package and in the Oracle Database Software release 8.1.6. A vulnerability has been found in the oidldap binary within the package.

A buffer overflow exists in the oidldap binary, which is setuid oracle. When executed on the command line, the oidldap binary performs an unsafe check of the ORACLE_HOME environment variable. It is possible for a malicous user to execute shell code through the ORACLE_HOME environment variable, allowing

the user to inherit an euid of oracle. In a stock installation of Oracle 8.1.6, this could create a scenario which would allow a local user to compromise the integrity of a database.

- **Oracle July Security Update Multiple Vulnerabilities**

Various Oracle Database Server, Oracle Enterprise Manager, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business Suite and Applications, Oracle Workflow, Oracle Forms and Reports, Oracle JInitiator, Oracle Developer Suite, and Oracle Express Server are affected by multiple vulnerabilities.

The issues identified by the vendor affect all security properties of the Oracle products and present local and remote threats.

Oracle has released a Critical Patch Update advisory for July 2005 to address these vulnerabilities. This Critical Patch Update addresses the vulnerabilities for supported releases. Earlier, unsupported releases are likely to be affected by the issues as well.

- **Oracle Listener Malformed Debugging Command Denial Of Service Vulnerability**

The Oracle Listener includes support for a number of debugging commands. These may be used by a remote administrator to retrieve information about the database.

The Oracle Listener process may crash when processing a malformed debugging request. A remote attacker may exploit this vulnerability to create a denial of service condition.

It has been reported that the debugging features in question are enabled by default, and may not be disabled through configuration.

- **Oracle Multiple Unspecified Vulnerabilities**

It is reported that multiple unspecified Oracle products contain multiple unspecified vulnerabilities.

The reported vulnerabilities include SQL injection, buffer overflows, and others.

There have also been reports that issues covered in this BID and resolved in the referenced Oracle patch include trigger abuse issues, character set conversion bugs and denial of service vulnerabilities. More information is pending.

It is noted that a number of unsupported versions of affected products may also potentially be vulnerable.

- **Oracle Multiple Vulnerabilities**

Oracle Database Server, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business and Applications, Oracle Enterprise Manager Grid Control,

and Oracle PeopleSoft Applications are reported prone to multiple vulnerabilities.

Oracle has released a Critical Patch Update to address these issues in various supported applications and platforms. Other non-supported versions may be affected, though this has not been confirmed by Symantec.

The issues identified by the vendor affect all security properties of the Oracle products and present local and remote threats. Various levels of authorization is required to leverage some issues, however, others do not require any authorization.

This BID will be divided and updated into separate BIDs when more information is available.

- **Oracle Net Listener Format String Vulnerability**

A vulnerability has been reported for the Listener Control utility (LSNRCTL). Reportedly, the Listener Control utility is vulnerable to format string attacks. This vulnerability is due to the default configuration of the Oracle Listener. The Listener, by default, allows users to modify configuration files without authenticating. It is possible for an attacker to modify certain entries in the file, listener.ora, to insert a format string exploit.

An attacker exploiting this vulnerability may obtain control over the Listener Control utility.

- **Oracle Net Services Link Buffer Overflow Vulnerability**

A buffer overflow vulnerability has been reported for Oracle Database Server. The vulnerability exists due to insufficient boundary checks performed on the CREATE DATABASE LINK query.

Successful exploitation will result in the corruption of sensitive stack memory to execute attacker-supplied code with the privileges of the database server.

- **Oracle OTRCREP Oracle Home Environment Variable Buffer Overflow Vulnerability**

Oracle is an Enterprise level SQL database, supporting numerous features and options. It is distributed and maintained by Oracle Corporation.

A buffer overflow has been discovered in the handling of $ORACLE_HOME by otrcrep. otrcrep is installed with the Oracle suite as a SUID oracle SGID dba binary. This buffer overflow may be exploited by a local user to overwrite stack variables, including the return address, and execute arbitrary code with the privileges of user oracle and group dba.

- **Oracle October Security Update Multiple Vulnerabilities**

Various Oracle Database Server, Oracle Enterprise Manager, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business Suite and Applications,

and Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne are affected by multiple vulnerabilities.

The issues identified by the vendor affect all security properties of the Oracle products and present local and remote threats.

Oracle has released a Critical Patch Update advisory for October 2005 to address these vulnerabilities. This Critical Patch Update addresses the vulnerabilities for supported releases. Earlier, unsupported releases are likely to be affected by the issues as well.

Specific details regarding these vulnerabilities are not currently available.

This record will be updated and split into individual BIDs for each issue as further information is disclosed.

- **Oracle RDBMS Server Default Account Vulnerability**

Oracle RDBMS Server is a fully-featured relational database management system. Oracle RDBMS provides a set of administrative tools for the Oracle database. Oracle is available for the Unix, Linux, and Microsoft Windows platforms.

In default installations of the Oracle database, the RDBMS Server installs a number of "demo" accounts with preset passwords. Remote attackers who are aware of the default accounts may use them to gain unauthorized access to the database.

Some of these default accounts are required by the database, others present a security vulnerability.

This has been a known issue for quite some time.

- **Oracle SQL*Plus Unauthorized Shell Command Execution Vulnerability**

Oracle Server is a fully-featured relational database management system.

SQL*Plus is the primary interface for the Oracle server, it integrates Oracle SQL and PL/SQL. SQL*Plus enables the retrieval and modification of data and the general maintenance of the database. Oracle is available for the Unix, Linux, and Microsoft Windows platforms.

Under the default settings, any connected SQL*Plus user may execute arbitrary shell commands.

- **Oracle TNS Listener Service_CurLoad Remote Denial Of Service Vulnerability**

The Oracle TNS Listener program is a remote connectivity service for Oracle Databases.

Under some circumstances, it may be possible for a remote user to crash TNS Listener service. By connecting to the service, and issuing the

SERVICE_CURLOAD command, the service becomes unstable. It has been reported that this will cause the listenering to stop responding to connections, and also crash after the command is issued.

- **Oracle XSQL Servlet Arbitrary Java Code Vulnerability**

The Oracle database server exhibits a possible failure to validate user-supplied input in stylesheet references contained in URLs submitted to the server.

Properly exploited, this may allow remote execution of arbitrary Java code with the webserver's privilege level.

- **Oracle cmctl Buffer Overflow Vulnerability**

Cmctl is the Connection Control Manager, part of the Oracle 8i installation. A vulnerability exists that can allow elevation of privileges.

The problem occurs in the way cmctl handles the user-supplied command line arguments. The string representing argv[1] (the first user-supplied commandline argument) is copied into a buffer of predefined length without being checked to ensure that its length does not exceed the size of the destination buffer. As a result, the excessive data that is written to the buffer will write past its boundaries and overwrite other values on the stack (such as the return address).

This can lead to the user executing supplied shellcode with the effective privileges of cmctl, egid dba and euid oracle.

- **Oracle for Linux Installer Vulnerability**

A vulnerability exists in the installation program for Oracle 8.1.5i. The Oracle installation scripts will create a directory named /tmp/orainstall, owned by oracle:dba, mode 711. Inside of this directory it will create a shell script named orainstRoot.sh, mode 777. The installation script will then stop and ask the person installing to run this script. The installation program at no point attempts to determine if the directory or script already exist. This makes it possible to create a symbolic link from the orainstRoot.sh file to elsewhere on the file system. This could be used to create a .rhosts file, for instance, and gain access to the root account. In addition, since the orainstRoot.sh file is mode 777, it is possible for any user on the machine to edit this script to execute arbitrary commands when run by root. Again, this can result in the compromise of the root account.

It is not readily apparent what versions of Oracle this does and does not affect. It has been confirmed on Oracle 8.1.5i, on the Linux/Intel platform. It is likely that this vulnerability may exists in other versions, and on other platforms. If you have any information about this, please mail us at: vuldb@securityfocus.com.

- **PHP .htaccess Attribute Transfer Vulnerability**

PHP the Personal Home Page software package distributed and maintained by the PHP Development Team. PHP provides enhanced attributes and added functionality to web pages.

A problem with the PHP package could allow for unauthorized access to restricted resources. The problem is specifically in the Apache Module of the PHP package, and affects the package only when running in combination with Apache Webserver. Per directory access control is done via the .htaccess file. However, by generating a custom crafted request, it is possible to force PHP to serve the next page with the same access control attributes as the previous accessed page. This problem could allow a malicious user to access restricted information in an intelligence gathering attack.

- **PHP 5 User-Supplied Session ID Input Validation Vulnerability**

PHP 5 is prone to an input-validation vulnerability. This is due to a lack of proper sanitization of user-supplied input of PHP session IDs, transmitted by way of HTTP headers.

An attacker may use this vulnerability to perform HTTP response splitting, often resulting in content spoofing and cross-site scripting attacks.

PHP 5 version 5.1.1 and prior are affected.

- **PHP Apache 2 Local Denial of Service Vulnerability**

PHP is prone to a local denial-of-service vulnerability when it is used as an Apache 2 module.

Reports indicate that due to a bug in the apache2handler SAPI (of the 'sapi_apache2.c' file), this issue triggers a segmentation fault and leads to a crash in the server.

This issue affects PHP versions prior to 5.1.0 final and 4.4.1 final.

- **PHP Apache 2 Virtual() Safe_Mode and Open_Basedir Restriction Bypass Vulnerability**

PHP on Apache 2 is prone to a restriction bypass vulnerability when calling 'virtual()'. Successful exploitation could lead to disclosure of sensitive information.

This issue is reported to affect PHP versions 4.4.0 and 5.0.5; other versions may also be vulnerable.

- **PHP DLOpen Memory Disclosure Vulnerability**

A vulnerability has been reported to present itself in the dlopen() function contained in the PHP source. The issue occurs when PHP is used in conjunction with the Apache web server. A local attacker may exploit this issue to gain unauthorized access to potentially sensitive information.

- **PHP Engine Disable Source Viewing Vulnerability**

PHP is the Personal Home Page package developed and maintained by the PHP Development Team. It is an open source, freely available, widely deployed package designed to enhance website content.

A problem in the package could allow external users to view the source code of PHP scripts. This problem is due to a bug in the PHP code, combined with a system using Apache and PHP and hosting several virtual hosts. When the PHP software is installed and turned off via configuration parameter "engine = off", it is possible for this configuration to affect not only the intended virtual host, but all virtual hosts managed by the system. In the event of such a configuration, it is possible for a malicious user to attain the source of various PHP scripts, which could lead to intelligence gathering and attack. This problem affects the PHP 4.x series on Apache Webserver only, and does not affect the PHP 3.x series.

- **PHP Error Logging Format String Vulnerability**

PHP is a scripting language designed for CGI applications that is used on many websites. There exists a remotely exploitable format string vulnerability in all versions of PHP below PHP 4.0.3.

The vulnerability exists in the code that handles error logging and is present if error logging is enabled in the "php.ini" configuration file. When errors are encountered by PHP, a string containing data supplied by the user is passed as the format string argument (the log_message variable) to the php_syslog() function (which contains *printf functions). As a result, it is possible for a malicious user to craft a string containing malicious format specifiers that will be passed to the php_syslog function as part of an error message. When interpreted by the *printf functions, these specifiers can cause the process to overwrite its own stack variables with arbitrary data. This can lead to remote access being gained on the target host with privileges of the webserver for the attacker.

Error logging may or may not be enabled by default on systems shipped with PHP.

- **PHP File Upload GLOBAL Variable Overwrite Vulnerability**

PHP is susceptible to a vulnerability that allows attackers to overwrite the GLOBAL variable via HTTP POST requests.

By exploiting this issue, remote attackers may be able to overwrite the GLOBAL variable. This may allow attackers to further exploit latent vulnerabilities in PHP scripts.

- **PHP Function CRLF Injection Vulnerability**

PHP includes a number of functions, such as fopen() and file(), which are used to reference external resources, such as other PHP files. If the allow_url_fopen() PHP directive is enabled, these functions may be used to access resources that exist on remote hosts by supplying a URL as an argument to the function. When these functions are used to reference a remote resource, PHP constructs a request for the resource using the appropriate protocol.

A vulnerability has been discovered in PHP which may allow an attacker to add arbitrary data to headers constructed by PHP when remote resources are referenced using these functions. In this way, a PHP script which uses the vulnerable function with the allow_url_fopen() directive enabled may be turned into a proxy, since the attacker is able to construct an arbitrary header to be sent with the request. This may be accomplished by building an arbitrary header using CRLF injection.

- **PHP Glob Function Local Information Disclosure Vulnerability**

A local information disclosure vulnerability affects PHP. This issue is due to a design error that presents potentially sensitive information to users within error messages.

An attacker may leverage this issue to reveal filenames and therefore the existence of files on an affected computer.

- **PHP Group Exif Module IFD Nesting Denial Of Service Vulnerability**

PHP is prone to a denial of service vulnerability. This issue occurs when deeply nested EXIF IFD (Image File Directory) data is processed.

This issue could manifest itself in Web applications that allow users to upload images.

This vulnerability may be one of the issues described in BID 13143 "PHP Group PHP Multiple Unspecified Vulnerabilities".

- **PHP Group Exif Module IFD Tag Integer Overflow Vulnerability**

PHP is prone to an integer overflow vulnerability in the EXIF module. This issue is exposed when malformed IFD (Image File Directory) tags are processed.

This issue could manifest itself in Web applications that allow users to upload images. Any other application that processes untrusted EXIF image data could also be exposed to attacks. Successful exploitation may allow for execution of arbitrary code.

This vulnerability may be one of the issues described in BID 13143 "PHP Group PHP Multiple Unspecified Vulnerabilities".

- **PHP Group Exif Module Infinite Recursion Denial Of Service Vulnerability**

PHP is prone to a denial-of-service vulnerability.

This issue occurs when parsing EXIF image data in corrupt JPEG files.

An attacker can exploit this vulnerability to crash the system, effectively denying service to legitimate users.

- **PHP Group PHP Image File Format Remote Denial Of Service Vulnerability**

A remote denial of service vulnerability affects PHP Group PHP. This issue is due to a failure of the application to properly handle maliciously formed Image Format File (IFF) image files.

It should be noted that this vulnerability can only be exploited remotely if a Web based PHP application is implemented that allows user-supplied images to be processed by the 'getimagesize()' function. The 'getimagesize()' is commonly implemented in PHP Web applications that allow for the display of images.

An attacker may leverage this issue to cause the affected script interpreter to consume excessive processing resources on an affected computer, leading to a denial of service condition.

- **PHP Group PHP Multiple Unspecified Vulnerabilities**

PHP is prone to multiple unspecified vulnerabilities.

PHP 5.0.3 and 4.3.10 are reported to be vulnerable. Earlier versions may also be affected.

- **PHP Group PHP Remote JPEG File Format Remote Denial Of Service Vulnerability**

A remote denial of service vulnerability affects PHP Group PHP. This issue is due to a failure of the application to properly handle maliciously crafted JPEG image files.

It should be noted that this vulnerability can only be exploited remotely if a Web based PHP application is implemented that allows user-supplied images to be processed by the 'getimagesize()' function. The 'getimagesize()' is commonly implemented in PHP Web applications that allow for the display of images.

An attacker may leverage this issue to cause the affected script interpreter to consume excessive processing resources on an affected computer, leading to a denial of service condition.

- **PHP Header Function Script Injection Vulnerability**

PHP is a freely available, open source web scripting language package. It is available for Microsoft Windows, Linux, and Unix operating systems.

It has been reported that a vulnerability in the PHP header function exists. It may be possible for a user to supply arbitrary script code in an URL that would allow the injection of script code into the HTTP header.

- **PHP Include File Relative Directory Information Disclosure Vulnerability**

Apache is a powerful, widely used web server available for most operating systems, including Linux, Windows and many other Unix like systems. PHP is a widely deployed scripting language, designed for web based development and CGI programming.

A path disclosure vulnerability exists in the default configuration of some releases of PHP when used with the Apache web server. If PHP include files are references with a relative directory, it is possible to cause the include statement to fail. Submitting a request for a php file appended with a trailing slash '/', will return an error message and the full path to the include file directory.

'Require' statements may also be susceptible to this issue.

- **PHP Input/Output Wrapper Remote Include Function Command Execution Weakness**

PHP is reportedly affected by an arbitrary command-execution weakness through the PHP 'include()' function. This issue is due to a design error that allows the execution of attacker-supplied POST PHP commands when URI data is used as an argument to an 'include()' function.

This issue affect the PHP module itself; however, the problem presents itself only when an application uses a user-supplied URI parameter as an argument to the 'include()' function.

This issue is reported to affect all versions of PHP since 3.0.13. Furthermore, this issue is not resolved by setting the 'php.ini' variable 'allow_url_fopen' to off.

Successful exploitation of this issue will allow an attacker to execute arbitrary PHP code on the affected computer; this will allow the execution of commands to the underlying operating system with the privileges of the affected webserver process.

- **PHP Interpreter Direct Invocation Denial Of Service Vulnerability**

It is possible, under some circumstances, for remote attackers to invoke the PHP interpreter from the web. If the interpreter is invoked with no command line options, it will hang. Attackers may exploit this condition to cause a denial of service.

This is reported to be a problem with PHP and Apache on Microsoft Windows platforms. It may be possible to create this condition in other environments as well.

- **PHP JPEG Image Buffer Overflow Vulnerability**

It is reported that PHP is susceptible to a buffer overflow vulnerability in handling JPEG images. This issue is due to a failure of the application to properly bounds check user-supplied image data prior to copying it into a fixed-size memory buffer.

This vulnerability allows remote attackers to alter the proper flow of execution of the application, potentially resulting in the execution of attacker-supplied machine code in the context of the web server executing the PHP interpreter.

- **PHP MB_Send_Mail TO Argument Header Injection Vulnerability**

PHP is susceptible to a header injection vulnerability when sending email. This issue is due to a failure of the application to properly sanitize user-supplied input.

This issue allows remote attackers to add arbitrary headers to generated email messages. The results of this vary depending on the meaning of the injected headers. This may allow attackers to utilize vulnerable Web applications as an anonymous email proxy.

- **PHP Microsoft Windows Shell Escape Functions Command Execution Vulnerability**

PHP is reportedly prone to a command execution vulnerability in its shell escape functions. This issue is due to a failure of PHP to properly sanitize function arguments.

This issue might allow an attacker to execute arbitrary shell commands on a computer running the vulnerable software within the security context of the web server; potentially leading to unauthorized access. Other attacks are also possible.

This issue is reported to affect PHP under Microsoft Windows version 4.3.3 and 4.3.5, it is likely that other Microsoft Windows versions are affected as well.

- **PHP Move_Uploaded_File Open_Basedir Circumvention Vulnerability**

PHP is a server side scripting language, designed to be embedded within HTML files. It is available for Windows, Linux, and many Unix based operating systems. It is commonly used for web development, and is very widely deployed.

It has been reported that the move_uploaded_file function lacks an open_basedir check. The effect of this issue is that this function may be used to perform file operations on directories outside of those specified by the open_basedir setting.

This vulnerability may not be exploited to overwrite existing files.

- **PHP Multiple Local And Remote Vulnerabilities**

PHP4 and PHP5 are reported prone to multiple local and remote vulnerabilities that may lead to code execution within the context of the vulnerable process. The following specific issues are reported:

A heap-based buffer overflow is reported to affect the PHP 'pack()' function call. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to execute arbitrary instructions in the context of the vulnerable process.

A heap-based memory disclosure vulnerability is reported to affect the PHP 'unpack()' function call. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to reveal portions of the process heap.

PHP safe_mode_exec_dir is reported prone to an access control bypass vulnerability. A local attacker that can manipulate the directory name from which the PHP script is called, may bypass 'safe_mode_exec_dir' restrictions by placing shell metacharacters and restricted commands into the directory name of the current directory.

PHP safe_mode is reported prone to an access control bypass vulnerability. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to execute commands that are otherwise restricted by PHP safe_mode.

PHP is reported prone to a 'realpath()' path truncation vulnerability. The vulnerability exists due to a lack of sanitization as to whether a path has been silently truncated by the libc realpath() function or not. This may lead to remote file include vulnerabilities in some cases.

The PHP function 'unserialize()' is reported prone to a memory corruption vulnerability. This corruption may be leveraged by a remote attacker that has the ability to make the PHP interpreter run a malicious script to execute arbitrary code in the context of the vulnerable process.

The PHP function 'unserialize()' is also reported prone to an information disclosure vulnerability. This issue may be leveraged by a remote attacker to disclose the contents of heap memory. This may allow them to gain access to potentially sensitive information, such as database credentials.

Finally, the PHP function 'unserialize()', is reported prone to an additional vulnerability. It is reported that previous versions of this function allow a malicious programmer to set references to entries of a variable hash that have already been freed. This can lead to remote memory corruption.

- **PHP Multiple Remote Vulnerabilities**

PHP4 and PHP5 are reported prone to multiple remotely exploitable vulnerabilities. These issue result from insufficient sanitization of user-supplied data. A remote attacker may carry out directory traversal attacks to disclose arbitrary files and upload files to arbitrary locations.

It is reported that these vulnerabilities may only be exploited on Windows.

- **PHP MySQLI Error Logging Remote Format String Vulnerability**

PHP is susceptible to a remote format string vulnerability in the 'mysqli' extension. This issue is due to a failure of the application to properly sanitize user-supplied input prior to using it in the format-specifier argument to a formatted printing function.

This issue allows attackers to execute arbitrary machine code in the context of the Web server hosting the PHP interpreter.

This issue affects PHP 5.1.0, and 5.1.1.

- **PHP MySQL_Connect Remote Buffer Overflow Vulnerability**

PHP is prone to a remote buffer overflow vulnerability.

An attacker can exploit this issue to execute arbitrary machine code in the context of the affected Web server. Failed exploit attempts will likely result in crashing the Web server, denying service to legitimate users.

It should be noted that arguments to the 'mysql_connect' function are not usually accessible for modification by remote attackers. This may limit the possible exploitation to legitimate users and administrators in a shared hosting environment.

PHP for Microsoft Windows versions 4.3.10, 4.4.0, and 4.4.1 are vulnerable; other versions may also be affected.

- **PHP Open_BaseDir Security Restriction Bypass Vulnerability**

PHP is prone to a vulnerability regarding the unauthorized access to directories outside the base directory.

The problem presents itself in the way PHP handles the 'open_basedir' directive.

Successful exploitation will grant an attacker access to directories outside the designated base directory. As a result, the attacker may access possibly privileged information.

This issue is reported to affect PHP versions 4.4.0 and 5.0.5; other versions may also be vulnerable.

- **PHP PHPInfo Cross-Site Scripting Vulnerability**

PHP is prone to a cross-site scripting vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input.

An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. This may facilitate the theft of cookie-based authentication credentials as well as other attacks.

- **PHP PHP_Variables Remote Memory Disclosure Vulnerability**

A vulnerability is reported to present itself in the array parsing functions of the 'php_variables.c' PHP source file.

The vulnerability occurs when a PHP script is being used to print URI parameters or data, that are supplied by a third party, into a dynamically generated web page. It is reported that the vulnerable function does not strip certain characters from the user supplied data, this may ultimately be harnessed to manipulate the parsing function into returning regions of process memory to the attacker.

It is reported that this issue only affects PHP versions 4.2.0 and subsequent.

- **PHP Parse_Str Register_Globals Activation Weakness**

PHP is susceptible to a weakness that allows attackers to reenable the 'register_globals' directive. This issue is due to the application's failure to handle a memory-limit exception.

The 'register_globals' directive will remain enabled for the rest of the lifetime of the affected process. If PHP is being run as an Apache module, then the process handling the malicious request will have 'register_globals' enabled for the duration of the process's life. If PHP is being run as a CGI process, this issue is not likely exploitable.

By exploiting this issue, remote attackers may be able to enable 'register_globals'. This may allow attackers to further exploit latent vulnerabilities in PHP scripts.

- **PHP Remote Arbitrary Location File Upload Vulnerability**

Reportedly PHP is vulnerable to an arbitrary location file upload vulnerability. This issue is due to a failure of the PHP application to properly sanitize user-supplied file name input.

An attacker may exploit this issue to upload files to an arbitrary location on a computer running the affected software. This may facilitate arbitrary server-side script code execution as well as other attacks.

It is reported that this issue only affects PHP versions 4.2.0 and subsequent.

- **PHP Safedir Restriction Bypass Vulnerabilities**

PHP is prone to multiple vulnerabilities that permit an attacker to bypass the 'safedir' directory restriction.

An attacker can exploit these vulnerabilities to possible execute arbitrary code currently existing on a vulnerable system, or to retrieve the contents of arbitrary files, all in the security context of the Web server process.

Information obtained may aid in further attacks against the affected system; other attacks are also possible.

These issues have been addressed in the latest CVS version.

- **PHP Session Handling Local Session Hijacking Vulnerability**

PHP is prone to a vulnerability that permits local hijacking of session variables. The problem presents itself in the way PHP stores session variables.

This issue can be exploited to hijack the session variables of victim users of other PHP applications running on a system utilizing a vulnerable version of PHP.

This issue is reported to effect the 3.x and 4.x versions of PHP; other versions may also be affected.

- **PHP Shared Memory Module Offset Memory Corruption Vulnerability**

PHP shared memory module (shmop) is reported prone to an integer handling vulnerability. The issue exists in the PHP_FUNCTION(shmop_write) function and is as a result of a lack of sufficient sanitization performed on 'offset' data.

This vulnerability may be exploited to make an almost arbitrary write into process memory. It is reported that the vulnerability may be leveraged to disable PHP 'safe mode', this may result in further compromise in a shared-server environment.

- **PHP Undefined Safe_Mode_Include_Dir Safemode Bypass Vulnerability**

PHP is prone to an issue that may allow programs to bypass Safe Mode by calling external files in restricted directories using include() and require().

The problem is known to occur when the safe_mode_include_dir PHP directive is not defined. A logic error reportedly exists which could result in PHP failing to run a security check when attempting to access a file via an include() or require() call, potentially bypassing the Safe Mode model. This could allow unauthorized access or policy bypass in environments that use Safe Mode, such as in cases where a web server resource is shared by multiple users.

This issue is reported to exist in PHP versions 4.3.0 and later.

- **PHP cURL Open_Basedir Restriction Bypass Vulnerability**

It is reported that cURL allows malicious users to bypass 'open_basedir' restrictions in PHP scripts. This issue is due to a failure of the cURL module to properly enforce PHPs 'open_basedir' restriction.

Users with the ability to create or modify PHP scripts on a server computer hosting the vulnerable software can reportedly exploit this vulnerability to bypass the 'open_basedir' restriction, and access arbitrary files with the privileges of the web server. This may aid them in further attacks.

This vulnerability possibly results in a false sense of security, as administrators expect that the restrictions in place prevent malicious users from gaining access to sensitive information.

- **PHP cURL and GD Multiple Safe_Mode and Open_Basedir Restriction Bypass Vulnerabilities**

PHP cURL and GD are prone to multiple safe_mode and open_basedir restriction-bypass vulnerabilities. Successful exploitation could lead to disclosure of sensitive information.

This issue is reported to affect PHP versions 4.4.0 and 5.0.5; other versions may also be vulnerable.

- **PHP posix_getpwnam / posix_getpwuid safe_mode Circumvention Vulnerability**

PHP is a server side scripting language, designed to be embedded within HTML files. It is available for Windows, Linux, and many Unix based operating systems. It is commonly used for web development, and is very widely deployed.

PHP safe_mode and open_basedir do not restrict the usage of posix_getpwnam and posix_getpwuid, allowing malicious scripts to access information related to local users of the system. Brute force enumeration of all user accounts is possible.

- **PHP3 'safe_mode' Failure Vulnerability**

PHP Version 3.0 is an HTML-embedded scripting language. Much of its syntax is borrowed from C, Java and Perl with a couple of unique PHP-specific features thrown in. The goal of the language is to allow web developers to write dynamically generated pages quickly.

Because it runs on a webserver and allows for user implemented (and perhaps security relevant) code to be executed on it, PHP has built in a security feature called 'safe_mode' to control executed commands to the webroot environment which PHP operates in.

This is done by forcing any system call which executes shell commands to have their shell commands passed to the EscapeShellCmd() function which ensures the commands do not take place outside the webroot directory.

Under certain versions of PHP however, the popen() command fails to be applied to the EscapeShellCmd() command and as such users can possibly exploit PHP applications running in 'safe_mode' which make of use of the 'popen' system call.

- **PHP4 Base64_Encode() Integer Overflow Vulnerability**

PHP4 has been reported prone to a potential integer overflow vulnerability.

The issue is reported to present itself in the base64_encode() function that is distributed as part of the PHP4 API. Although unconfirmed it has been conjectured that this issue may be due to an unsigned integer value wrapping to a value of zero. This value may then be used in boundary controls, or in arithmetic that may potentially influence execution flow or result in the corruption of sensitive regions of memory.

It is currently unknown whether this condition is exploitable or not.

- **PHP4 Multiple Vulnerabilities**

PHP have released an upgrade to address multiple vulnerabilities, including integer overflow issues that have been reported to affect PHP4 and bundled software.

Exploitation of these issues may have varying impacts, although unconfirmed potentially resulting in a denial of service or ultimately arbitrary code execution.

This BID will be split up into individual BIDs as further analysis of these issues is completed.

- **PHP4 Readfile Denial Of Service Vulnerability**

PHP4 is reported prone to a denial of service vulnerability. It is reported that the PHP 'readfile()' function may be utilized to trigger this issue.

An attacker that has access to a PHP enabled web host may exploit this vulnerability to crash the HTTP server that is incorporating the vulnerable PHP module.

- **PHP4 Session Files Local Information Disclosure Vulnerability**

PHP is a server side scripting language, designed to be embedded within HTML files. It has been released for Windows, Linux, and many Unix based operating systems. It is commonly used for web development, and is very widely deployed.

PHP session information may be stored in files in the /tmp directory. These files are give names including the session ID. A local attacker may view the contents

of the /tmp directory and use the session IDs revealed to hijack current web sessions.

- **Sun Java Runtime Environment Java Plug-in JavaScript Security Restriction Bypass Vulnerability**

A vulnerability is reported to exist in the access controls of the Java to JavaScript data exchange within web browsers that employ the Sun Java Plug-in. Reports indicate that it is possible for a malicious website that contains JavaScript code to exploit this vulnerability to load a dangerous Java class and to pass this class to an invoked applet.

** UPDATE: It is reported that the various methods of invoking Java applets can be abused to specify which version of a plug-in will be used to run an applet. If a vulnerable version is still installed on the computer, it may be possible for to specify that this version runs the applet instead of an updated version that is not prone to the vulnerability. Users affected by this vulnerability should remove earlier versions of the plug-in. This functionality could also be abused to prompt users to install vulnerable versions of the plug-in, so users should be wary of doing so. This general security weakness has been assigned an individual BID (11757). It is not known to what degree the Sun Java Runtime Environment Java Plug-in JavaScript Security Restriction Bypass Vulnerability is affected by this security weakness, though a number of other known vulnerabilities could be affected.

- **WinMySQLadmin Plain Text Password Storage Vulnerability**

A vunerability exists in WinMySQLadmin 1.1 that may result in the disclosure of sensitive authentication information for MySQL.

If a local user gained access to the 'my.ini' file, it is possible to retrieve configuration and authentication information for MySQL. The contents of this file are in plain text.

- **Windows 2000 DCOM Client Memory Disclosure Vulnerability**

Microsoft Distributed Component Object Model (DCOM) can be used to support COM communication. A vulnerability has been reported with the DCOM client included with Windows 2000.

Under some circumstances, when the DCOM client sends a request, uninitialized memory is included in the transmitted data. This data is normally ignored by the server, having no impact on application performance. However, the data may include uninitialized areas of server memory, and lead to the disclosure of sensitive information.

At this time, the memory data disclosed is believed to be essentially random. An attacker must, at best, hope that sensitive information will be included in the client message by chance.

- **XML-RPC for PHP Remote Code Injection Vulnerability**

XML-RPC for PHP is affected by a remote code injection vulnerability.

An attacker may exploit this issue to execute arbitrary commands or code in the context of the Web server. This may facilitate various attacks including unauthorized remote access.

XML-RPC for PHP 1.1 and prior versions are affected by this issue. Other applications using this library are also affected.

- **Zlib Compression Library Buffer Overflow Vulnerability**

Zlib is susceptible to a buffer-overflow vulnerability. This issue is due to the application's failure to properly validate input data before using it in a memory copy operation.

In certain circumstances, malformed input data during decompression may result in a memory buffer being overflowed. This may result in denial-of-service conditions or may allow remote code to execute in the context of applications that use the affected library.

Security Update 27

Symantec NetRecon 3.6 Security Update 27 (SU27) detects and reports 119 new vulnerabilities.

New vulnerability detection

- **Cisco Internet Operating System SNMP Message Processing Denial Of Service Vulnerability**

It has been reported that the Cisco Internet Operating System (IOS) is affected by a remote SNMP message processing denial of service vulnerability. This is caused by a design error that causes memory corruption in the affected system under certain circumstances.

This issue may be leveraged to cause a denial of service condition in the affected device. The denial of service is due to a corruption of memory in the affected device. As a result, there may be other consequences, such as code execution. This has not been confirmed by Cisco.

- **Apache mod_auth Malformed Password Potential Memory Corruption Vulnerability**

It has been reported that Apache may be prone to a memory corruption vulnerability when parsing malformed password values during authentication. The issue is reported to exist in the authentication modules (mod_auth,

mod_auth3, mod_auth4) employed by Apache. All versions of Apache running on 16-bit and 64-bit systems could potentially be vulnerable to this issue.

- **Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability**

A stack-based buffer overflow has been reported in the Apache mod_ssl module.

This issue is exposed in utility code for uuencoding binary data.

This issue would most likely result in a denial of service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures.

- **Apache Mod_Proxy Remote Negative Content-Length Buffer Overflow Vulnerability**

A remote buffer overflow vulnerability exists in Apache mod_proxy.

The source of this issue is that a negative user-specified length value may be used in a memory copy operation, allowing for corruption of memory. This may triggered if a remote server returns a negative Content-Length: HTTP header field to be passed through the proxy.

Exploitation will likely result in a denial of service, though there is an unconfirmed potential for execution of arbitrary code on some platforms (such as BSD implementations). Versions that have the optional AP_ENABLE_EXCEPTION_HOOK define enabled may also be exploitable on some platforms.

This issue affects Apache servers 1.3.26 through 1.3.32 that have mod_proxy enabled and configured. Apache 2.0.x releases are not affected by this issue.

- **Cisco IOS Border Gateway Protocol Denial Of Service Vulnerability**

The problem presents itself when an affected device handles a malformed or invalid Border Gateway Protocol (BGP) packet. During processing the offending packet the affected device will reset.

It should be noted that this issue only affects devices with BGP enabled; BGP is not enabled by default. It has been reported that this issue would be very difficult to exploit as it would require injecting malicious packets into communication between trusted peers.

An attacker may exploit this issue to cause the affected device to reset, taking several minutes to become functional. It is possible to create a persistent denial of service condition by continually transmitting malformed packets to the affected device.

- **Apache mod_userdir Module Information Disclosure Vulnerability**

It is reported that the Apache mod_userdir module is prone to an information disclosure vulnerability. The issue is reported to exist because the module is configured in an insecure manner by default.

It is reported that an attacker may exploit this vulnerability to harvest user account usernames that are present on the affected host.

- **Cisco IOS OSPF Remote Denial Of Service Vulnerability**

Cisco IOS is reported prone to a remote denial of service vulnerability.

It is reported that the vulnerability manifests when a malformed Open Shortest Path First (OSPF) packet is handled by the vulnerable router.

A remote attacker may exploit this condition in multiple routers that reside on the same network segment as the attacker, to trigger a device reset. The attacker may continuously transmit malicious OSPF packets to the target routers in order to effectively deny network services to legitimate hosts.

- **Apache mod_ssl Remote Denial of Service Vulnerability**

Apache 2.x mod_ssl is reported prone to a remote denial of service vulnerability. This issue likely exists because the application fails to handle exceptional conditions. The vulnerability originates in the 'char_buffer_read' function of the 'ssl_engine_io.c' file.

It is likely that this issue only results in a denial of service condition in child process. This BID will be updated as more information becomes available.

Apache 2.0.50 is reported to be affected by this issue, however, it is possible that other versions are vulnerable as well.

- **Apache Mod_DAV LOCK Denial Of Service Vulnerability**

Apache's 'mod_dav' module is reported susceptible to a denial of service vulnerability.

This vulnerability presents itself when Apache is configured to use the 'mod_dav' module, and it receives a specific sequence of LOCK commands from an authorized user.

This vulnerability can be exploited by remote attackers to crash Apache processes. If Apache is configured to use the threaded process model, an attacker could completely crash Apache. If Apache is configured to use multiple processes as apposed to threads, an attacker could crash individual web server processes. With a sustained attack, they could crash multiple server processes, and still likely deny service to legitimate users.

All versions of Apache 2.0, prior to 2.0.51 are reported vulnerable.

- **Apache Satisfy Directive Access Control Bypass Vulnerability**

Apache Web Server is reportedly affected by an access control bypass vulnerability. This issue presents itself due to an unspecified error in the merging of the 'Satisfy' directive. As a result, a remote attacker may bypass access controls and gain unauthorized access to restricted resources.

It is reported that this issue only affects Apache 2.0.51.

Due to a lack of details, further information is not available at the moment. This BID will be updated as more information becomes available.

- **Apache mod_ssl SSLCipherSuite Restriction Bypass Vulnerability**

Apache 2.x mod_ssl is reported prone to a restriction bypass vulnerability. This issue presents itself when mod_ssl is configured to be used with the 'SSLCipherSuite' directive in 'Directory' or 'Location' context. It is reported that this vulnerability allows a client to use any cipher suite allowed by the virtual host configuration regardless of cipher suites specified for a specific directory. This can allow an attacker to bypass security policies and utilize potentially weaker encryption types than allowed.

Apache versions 2.0.35 to 2.0.52 are reported vulnerable to this issue.

- **Apache mod_include Local Buffer Overflow Vulnerability**

The problem presents itself when the affected module attempts to parse mod_include specific tag values. A failure to properly validate the lengths of user-supplied tag strings prior to copying them into finite buffers facilitates the overflow.

A local attacker may leverage this issue to execute arbitrary code on the affected computer with the privileges of the affected Apache server.

- **Cisco IOS DHCP Input Queue Blocking Denial Of Service Vulnerability**

Cisco IOS is reported susceptible to a remote denial of service vulnerability when handling specific DHCP packets.

Reportedly, DHCP packets containing certain unspecified content have the capability to block the input queue of interfaces on affected devices.

Once an input queue is blocked, further ARP, and routing protocol packets will not be processed. This condition can only be corrected by rebooting the affected device.

An attacker with the ability to send malicious DHCP packets to an affected device may be able to interrupt the routing services of the affected device, potentially denying further network service to legitimate users.

- **Microsoft Windows FTP Client Directory Traversal Vulnerability**

Microsoft Windows FTP client is reported prone to a directory traversal vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied input. A remote attacker may place files in an arbitrary location on a vulnerable computer.

This can lead to data corruption or creation of potentially malicious files on a vulnerable computer. Once the file is placed on the computer, the attacker can employ various methods to execute the file or use this issue to aid in further attacks against a vulnerable computer. This would occur in the context of the user running Internet Explorer.

- **Apache Utilities Insecure Temporary File Creation Vulnerability**

A local insecure temporary file creation vulnerability reportedly affects Apache Software Foundation Apache Utilities. This issue is due to a failure of the affected utility to securely create temporary files in world writable locations.

An attacker may leverage this issue to corrupt, write to or create arbitrary files with the privileges of the user or process running the vulnerable script.

- **Cisco IOS IPv6 Processing Remote Denial Of Service Vulnerability**

A remote denial of service vulnerability affects the IPv6 processing functionality of Cisco IOS. This issue is due to a failure of the affected operating system to properly handle specially crafted network data.

It is possible for an attacker to produce a sustained denial of service condition against an affected device by continually sending the malicious network data.

An attacker may leverage this issue to cause an affected device to reload, denying service to legitimate users.

- **Cisco IOS Multi Protocol Label Switching Remote Denial Of Service Vulnerability**

Cisco IOS based routers that are configured with support for Multi Protocol Label Switching (MPLS) are reported prone to a remote denial of service vulnerability.

It is reported that the vulnerability presents itself when an affected router handles an unspecified malicious packet on a MPLS disabled interface.

A remote attacker that resides on the same network segment as the vulnerable router may exploit this vulnerability continuously to effectively deny network-based services to legitimate users.

- **Cisco IOS Border Gateway Protocol Processing Remote Denial Of Service Vulnerability**

A remote denial of service vulnerability affects the Border Gateway Protocol (BGP) processing functionality of Cisco IOS. This issue is due to a failure of the application to handle malformed network data.

An attacker may leverage this issue to trigger a denial of service condition in the affected device. A persistent denial of service attack can be triggered as well.

- **Apache Tomcat Remote Malformed Request Denial Of Service Vulnerability**

A remote denial of service vulnerability affects Apache Tomcat. This issue is due to a failure of the application to properly handle malformed requests.

An attacker may leverage this issue to trigger a denial of service condition in the affected software.

- **Microsoft Windows Graphical Device Interface Library Denial Of Service Vulnerability**

Reportedly, a denial of service vulnerability affects Microsoft Windows GDI library 'gdi32.dll'. This issue is due to a failure of the application to securely copy data from malformed EMF image files.

An attacker may leverage this issue to trigger a denial of service condition in software implementing the vulnerable library. Other attacks may also be possible.

- **Apache mod_ssl ssl_io_filter_cleanup Remote Denial Of Service Vulnerability**

mod_ssl is prone to a remote denial of service vulnerability. The issue exists in the 'ssl_io_filter_cleanup' function.

A remote attacker can exploit this issue to cause a denial of service condition in an affected Apache server.

Apache 2.0.49 and prior versions are considered to be affected by this vulnerability.

- **TACACS+ Protocol Flaws Vulnerabilities**

A number of vulnerabilities exist in the TACACS+ protocol. These are part of the protocol, and as such do not affect only those products listed as being vulnerable, but any implementation of TACACS+, both on the client and on the server side.

1) Integrity Checking

TACACS+ does not use any form of integrity checking to ensure a TACACS+ packet has not been tampered with. Due to the nature of its encryption

mechanism, an attacker could potentially alter a packet by flipping bits. One example cited is the possibility of an attacker flipping a single bit to alter an accounting packet, changing the elapsed_time being reported from 9000 to 1000.

2) Vulnerability to Replay

TACACS+ has no protection against replay attacks. So long as a packet has the correct TACACS+ sequence number, it will be accepted. As TACACS+ sequence numbers start at 1, the server will always process packets with the sequence number of 1. The description of this vulnerability noted that this is most easily used against accounting packets, as they are single packet transactions.

3) Session ID collision

The encryption mechanism for TACACS+ depends heavily on a unique session_id for each session. If multiple sessions get the same session_id and seq_no, it can become vulnerable to a frequency analysis attack. In addition, if plaintext is known in one packet, it is trivial to decrypt the corresponding portion of the other packet containing the same sequence and session id. It is possible to get a TACACS+ server to encrypt a reply packet using a chosen session_id. This makes it possible to compromise the encryption of packets from the server to client.

4) Session ID randomness

Due to the length of the session_id, and an inability to prevent id collision across reboots and multiple servers, session id's will eventually be reused, which can result in the decryption of packets. For an ISP handling 20,000 dialup sessions a day, there could be over 100,000 session_id collisions in a year.

5) Lack of padding

A lack of padding of fields in the protocol can reveal the length of these unpadded fields. This could result in revealing the length of a user password.

6) MD5 context leak

A theoretical vulnerability exists whereby part of a packet may be decrypted, due to the presence of certain bytes.

These attacks all require the attacker be present on the network where these transaction are taking place; in some cases, the attack may need to be on a machine or router separating the client from the server. As such, while very real vulnerabilities, using them in a real world situation may be difficult.

- **Cisco IOS Easy VPN Server XAUTH Authentication Bypass Vulnerability**

Cisco IOS Easy VPN Server is reported prone to an authentication bypass vulnerability. This issue can allow remote attackers to bypass Extended Authentication (XAUTH) and gain unauthorized access to resources.

An unauthorized attacker may send certain malformed UDP packets to UDP port 500 to complete XAUTH authentication and gain unauthorized access to network resources.

- **Cisco IOS Unauthorized Security Association Establishment Vulnerability**

Cisco IOS is prone to an issue related to XAUTH and ISAKMP profiles that may allow a malicious VPN client to gain unauthorized access to a VPN.

The vulnerability occurs in a case where attributes in an ISAKMP profile that have been assigned to remote peer are not processed. This will present a window of opportunity for the remote client to initiate Phase 2 IKE negotiation and cause an unauthorized IPSec SA (Security Association) to be established.

It is noted that the vulnerability only affects those ISAKMP profiles that are matched by pre-configured certificate maps.

- **Cisco IOS Secure Shell Server Memory Leak Denial Of Service Vulnerability**

A denial of service vulnerability has been reported in the Cisco IOS Secure Shell Server implementation.

This condition is the result of a memory leak that may be triggered by remote clients under some circumstances. If the memory leak is triggered repeatedly, this could exhaust resources on the device, resulting in a reload of the device and persistent denial of service.

- **Cisco IOS Secure Shell Server V2 Remote Denial Of Service Vulnerability**

Cisco IOS is reported prone to a remote denial of service vulnerability. The issue is reported to exist when the Cisco IOS device is configured to employ SSHv2 for remote management and Terminal Access Controller Access Control System Authentication (TACACS+).

An attacker may trigger the issue to cause a device reload, effectively denying service for legitimate users.

It is noted that the vulnerability only affects SSHv2, SSHv1 is not affected.

- **Apache HTDigest Realm Command Line Argument Buffer Overflow Vulnerability**

A buffer overflow vulnerability exists in the htdigest utility included with Apache. The vulnerability is due to improper bounds checking when copying user-supplied realm data into local buffers.

By supplying an overly long realm value to the command line options of htdigest, it is possible to trigger an overflow condition. This may cause memory to be corrupted with attacker-specified values.

This issue could be exploited by a remote attacker; potentially resulting in the execution of arbitrary system commands within the context of the web server process.

- **Apache Tomcat Java Security Manager Bypass Vulnerability**

Apache Tomcat is susceptible to a Java Security Manager sandbox bypass vulnerability. The issue may be leveraged using the request dispatcher to bypass the Java Security Manager.

Information that is harvested through the exploitation of this vulnerability may be used to aid in further attacks.

- **Apache HTPasswd User Command Line Argument Buffer Overflow Vulnerability**

A buffer overflow vulnerability exists in the htpasswd utility included with Apache. The vulnerability is due to improper bounds checking when copying user-supplied 'user' data into local buffers.

Since the program is not setuid, this vulnerability does not have a local impact. However, this may be an issue if the software is called from a CGI script. An attacker may be able to supply malformed data to the program which will cause the overflow to occur.

- **Apache HTPasswd Password Command Line Argument Buffer Overflow Vulnerability**

A buffer overflow vulnerability exists in the htpasswd utility included with Apache. The vulnerability is due to improper bounds checking when copying user-supplied 'password' data into local buffers.

Since the program is not setuid, this vulnerability does not have a local impact. However, this may be an issue if the software is called from a CGI script. An attacker may be able to supply malformed data to the program which will cause the overflow to occur.

- **Microsoft Internet Explorer JavaScript OnLoad Handler Remote Code Execution Vulnerability**

Microsoft Internet Explorer is affected by a remote code execution vulnerability.

This vulnerability presents itself when the browser handles a JavaScript 'onLoad' handler in conjunction with an improperly initialized 'window()' JavaScript function.

This issue may be exploited to execute arbitrary remote code in the context of the user running the affected application. Failed exploitation attempts likely result in the application crashing.

- **Multiple Vendor Multiple HTTP Request Smuggling Vulnerabilities**

Multiple vendors are prone to a new class of attack named 'HTTP Request Smuggling'. This class of attack basically revolves around piggybacking a HTTP request inside of another HTTP request. By leveraging failures to implement the HTTP/1.1 RFC properly, it is demonstrated that this class of attack may result in cache poisoning, cross-site scripting, session hijacking and other attacks.

- **Cisco IOS AAA RADIUS Authentication Bypass Vulnerability**

Cisco IOS Remote Authentication Dial In User Service (RADIUS) is prone to a remote authentication bypass vulnerability.

The issue manifests when Cisco IOS is configured to employ AAA RADIUS authentication and is configured to use 'none' as a fallback method.

A remote attacker may exploit this issue to bypass authentication and gain unauthorized access to the affected service.

- **Apache HTTP Request Smuggling Vulnerability**

Apache is prone to an HTTP request smuggling attack.

A specially crafted request with a 'Transfer-Encoding: chunked' header and a 'Content-Length' can cause the server to forward a reassembled request with the original 'Content-Length' header. Due to this, the malicious request may piggyback with the valid HTTP request.

It is possible that this attack may result in cache poisoning, cross-site scripting, session hijacking and other attacks.

This issue was originally described in BID 13873 (Multiple Vendor Multiple HTTP Request Smuggling Vulnerabilities). Due to the availability of more details and vendor confirmation, it is being assigned a new BID.

- **Microsoft Windows Network Connections Manager Library Local Denial of Service Vulnerability**

netman.dll is affected by a local denial of service vulnerability.

A successful attack can cause a denial of service condition in the Network Connections Service.

Various services such as Wuauserv, Browser, CryptSvc, TrkWks, dmserver, seclogon, lanmanserver, ShellHWDetection, AudioSrv, WZCSVC and lanmanworkstation may also become inaccessible to the exploitation of this issue.

It should be noted on Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1, this issue is only available locally and an attacker must have valid logon credentials.

On Windows 2000, Windows XP Service Pack 1 and Windows Server 2003, an attacker must have valid logon credentials to exploit this vulnerability. The vulnerability can however be exploited remotely to users who have standard user accounts.

- **Apache mod_ssl CRL Handling Off-By-One Buffer Overflow Vulnerability**

mod_ssl is prone to an off-by-one buffer overflow condition.

The vulnerability arising in the mod_ssl CRL verification callback allows for potential memory corruption when a malicious CRL is handled.

An attacker may exploit this issue to trigger a denial of service condition. It is conjectured that arbitrary code execution may be possible as well.

- **Cisco IOS IPv6 Processing Arbitrary Code Execution Vulnerability**

A remote arbitrary code execution vulnerability affects the IPv6 processing functionality of Cisco IOS.

A successful attack may allow a remote attacker to execute arbitrary code and gain unauthorized access to the device. An attacker can also leverage this issue to cause an affected device to reload, denying service to legitimate users.

This issue may be related to BID 12368 (Cisco IOS IPv6 Processing Remote Denial Of Service Vulnerability).

Cisco has stated that exploitation of this vulnerability in Cisco IOS XR may cause the IPv6 neighbor discovery process to restart. If exploited repeatedly, this could result in a prolonged denial of service affecting IPv6 traffic travelling through the device.

- **Microsoft Visual Studio .NET msdds.dll Remote Code Execution Vulnerability**

Microsoft Visual Studio .NET is prone to a vulnerability that could allow remote arbitrary code execution. This is due to a buffer overflow that is exposed during COM object instantiation.

The list of vulnerable packages has been updated to include applications suspected of installing the vulnerable msdds.dll library.

- **PCRE Regular Expression Heap Overflow Vulnerability**

PCRE is prone to a heap overflow vulnerability. This issue is due to a failure of the library to properly bounds check user-supplied input prior to copying data to an internal memory buffer.

The impact of successful exploitation of this vulnerability depends on the application and the user credentials utilizing the vulnerable library. Successful attack may ultimately permit an attacker to control the contents of critical

memory control structures and write arbitrary data to arbitrary memory locations.

- **Apache CGI Byterange Request Denial of Service Vulnerability**

Apache is prone to a denial of service when handling large CGI byterange requests.

- **Apache Mod_SSL SSLVerifyClient Restriction Bypass Vulnerability**

Apache 2.x mod_ssl is prone to a restriction bypass vulnerability. This issue presents itself when mod_ssl is configured to be used with the 'SSLVerifyClient' directive.

This issue allows attackers to bypass security policies to gain access to locations that are configured to be forbidden for clients without a valid client certificate.

- **Cisco IOS Firewall Authentication Proxy Buffer Overflow Vulnerability**

Cisco IOS Firewall Authentication Proxy is prone to a buffer overflow condition. Successful exploitation of this issue could cause a denial of service or potential execution of arbitrary code.

This issue affects the FTP and Telnet protocols, but not HTTP.

- **Microsoft Windows MSDTC Memory Corruption Vulnerability**

The Microsoft Windows MSDTC (Microsoft Distribution Transaction Coordinator) service is prone to a memory corruption vulnerability. This issue could allow for execution of arbitrary code in the context of the service. The vulnerability may be remotely exploitable in some circumstances, but will also permit local privilege escalation.

This issue is remotely exploitable on Windows 2000 platforms, since the Network DTC is enabled by default on this platform. On Windows XP, this issue may be remotely exploitable if a local user has started the service. On Windows Server 2003, this vulnerability is limited to local privilege escalation unless Network DTC has been explicitly enabled by an administrator. This issue is not present on Windows XP SP2 and Windows Server 2003 SP1.

Update: Microsoft reports several systems have experienced one or more problems after installing the critical update from Microsoft Security Bulletin MS05-051 for this issue.

- **Microsoft MSDTC COM+ Remote Code Execution Vulnerability**

Microsoft Windows is prone to a vulnerability in the COM+ (Component Object Model) functionality of the MSDTC (Microsoft Distribution Transaction Coordinator) service. This issue may permit remote and local attackers to execute arbitrary code in the context of the service.

This issue may be exploited by remote anonymous attackers on Windows 2000 platforms. On Windows XP versions up to and including SP1, the attacker must authenticate as the Guest or another account prior to exploitation. On Windows XP SP2 and all Windows Server 2003 operating systems, this issue is limited to local privilege escalation.

Update: Microsoft reports several systems have experienced one or more problems after installing the critical update from Microsoft Security Bulletin MS05-051 for this issue. For a more detailed explanation of these problems please see the attached microsoft knowledge base article 909444.

- **Microsoft MSDTC TIP Denial Of Service Vulnerability**

The Microsoft Windows MSDTC (Microsoft Distribution Transaction Coordinator) service is prone to a denial of service vulnerability.

The vulnerability exists in the TIP (Transaction Internet Protocol) functionality that is provided by MSDTC. This vulnerability may be exploited by a remote attacker to deny the availability of services that depend on MSDTC.

This issue only exists on operating systems that have support for the TIP protocol enabled. This vulnerability is remotely exploitable on default configurations on Windows 2000. TIP is not enabled by default on Windows XP and Windows Server 2003 even if the MSDTC service is running.

Update: Microsoft reports several systems have experienced one or more problems after installing the critical update from Microsoft Security Bulletin MS05-051 for this issue. For a more detailed explanation of these problems please see the attached microsoft knowledge base article 909444.

- **Microsoft MSDTC TIP Distributed Denial Of Service Vulnerability**

The Microsoft MSDTC (Microsoft Distribution Transaction Coordinator) service is prone to a vulnerability that may permit denial of service attacks against the service or facilitate distributed denial of service attacks against other computers.

The vulnerability exists in the TIP (Transaction Internet Protocol) functionality that is provided by MSDTC.

This issue only exists on operating systems that have support for the TIP protocol enabled. This vulnerability is remotely exploitable on default configurations on Windows 2000. TIP is not enabled by default on Windows XP and Windows Server 2003 even if the MSDTC service is running.

Update: Microsoft reports several systems have experienced one or more problems after installing the critical update from Microsoft Security Bulletin MS05-051 for this issue. For a more detailed explanation of these problems please see the attached microsoft knowledge base article 909444.

- **Microsoft Internet Explorer COM Object Instantiation Variant Vulnerability**

Microsoft Internet Explorer is prone to a buffer overflow vulnerability that is related to instantiation of COM objects.

Successful exploitation could let remote attackers execute arbitrary code in the context of the currently logged in user on the affected computer.

This is a variant of the vulnerability described in BID 14511 Microsoft Internet Explorer COM Object Instantiation Buffer Overflow Vulnerability. The difference between this issue and BID 14511 is that a different set of COM objects are affected that were not addressed in the previous BID.

- **Microsoft DirectX DirectShow AVI Processing Buffer Overflow Vulnerability**

A buffer overflow vulnerability exists in the Microsoft Windows DirectX component. This issue is related to processing of .AVI (Audio Visual Interleave) media files. The specific vulnerability exists in DirectShow and could be exposed through applications that employ DirectShow to process .AVI files.

Successful exploitation will permit execution of arbitrary code in the context of the user who opens a malicious .AVI file.

This issue could be exploited through any means that will allow the attacker to deliver a malicious .AVI file to a victim user. In Web-based attack scenarios, exploitation could occur automatically if the malicious Web page can cause the .AVI file to be loaded automatically by Windows Media Player. Other attack vectors such as email or instant messaging may require the victim user to manually open the malicious .AVI.

It is not known if third-party applications rely on DirectShow to process .AVI files. If so, these applications could also present an attack vector.

- **Microsoft Windows Explorer Web View Script Injection Vulnerability**

Microsoft Windows Explorer Web View is affected by an arbitrary script injection vulnerability.

An attacker can exploit this issue by crafting a malicious file and placing it on a Web site or sending it to a user through email followed by enticing them to preview it in Windows Explorer.

A successful attack can result in a remote compromise in the context of the vulnerable user.

- **Microsoft Windows Plug And Play UMPNPMGR.DLL wsprintfW Buffer Overflow Vulnerability**

Microsoft Windows Plug and Play is prone to a buffer overflow vulnerability. This issue is due to a failure of the service to properly bounds check user-supplied data prior to copying it to an insufficiently sized memory buffer.

This issue takes place when the PnP service handles malformed messages containing excessive data.

This vulnerability facilitates local privilege escalation and unauthorized remote access depending on the underlying operating system. A successful attack may result in arbitrary code execution resulting in an attacker gaining SYSTEM privileges.

This issue is unrelated to BID 14513, Microsoft Windows Plug and Play Buffer Overflow Vulnerability, but they both have similar attack scenarios and affects.

- **Microsoft Windows Client Service For Netware Buffer Overflow Vulnerability**

Microsoft Client Service for Netware is prone to a buffer overflow vulnerability that could permit the execution of arbitrary remote code.

A remote attacker can exploit this vulnerability to execute arbitrary code and completely compromise the computer. This issue could also be exploited by local attackers to gain elevated privileges.

It should be noted that the Client Service for Netware is not installed by default on any affected operating system. Microsoft Windows XP Home is not affected by this vulnerability at all.

- **Microsoft Collaboration Data Objects Remote Buffer Overflow Vulnerability**

Microsoft CDO is susceptible to a remote buffer overflow vulnerability. This issue is due to a failure of the library to properly bounds check user-supplied data prior to copying it to an insufficiently sized memory buffer.

This issue presents itself when an attacker sends a specifically crafted email message to an email server utilizing the affected library.

This issue allows remote attackers to execute arbitrary machine code in the context of the application utilizing the library.

- **Microsoft Windows Malicious Shortcut Handling Remote Code Execution Vulnerability**

Microsoft Windows is prone to a remote code execution vulnerability when handling a malicious shortcut (.lnk) file.

An attacker can exploit this issue by crafting a malicious file and placing it on a Web site or sending it to a user through email followed by enticing them to open it and view the file's properties.

This issue also poses a local threat as a local unprivileged attacker could exploit this issue without user interaction to gain elevated privileges.

This vulnerability can facilitate arbitrary code execution with SYSTEM privileges.

This BID is related to the issue described in BID 15070 (Microsoft Windows Malicious Shortcut Handling Remote Code Execution Variant Vulnerability).

- **Microsoft Windows Malicious Shortcut Handling Remote Code Execution Variant Vulnerability**

Microsoft Windows is prone to a remote code execution vulnerability when handling a malicious shortcut (.lnk) file.

An attacker can exploit this issue by crafting a malicious file and placing it on a Web site or sending it to a user through email followed by enticing them to open it and view the file's properties.

This issue also poses a local threat as a local unprivileged attacker could exploit this issue without user interaction to gain elevated privileges.

This vulnerability can facilitate arbitrary code execution with SYSTEM privileges.

This BID is related to the issue described in BID 15069 (Microsoft Windows Malicious Shortcut Handling Remote Code Execution Vulnerability).

- **Cisco IOS System Timers Heap Buffer Overflow Exploitation**

Cisco IOS is prone to heap-based buffer overflow exploitation. Cisco has released an advisory stating that IOS upgrades are available to address the possibility of exploitation of heap-based buffer overflow vulnerabilities. It is not known at this time if the advisory addresses a specific heap overflow or just provides security enhancements to mitigate attempts to exploit other heap overflow vulnerabilities.

- **Apache Tomcat 3.1 Path Revealing Vulnerability**

A vulnerability exists in the JSP portion of the Tomcat package, version 3.1, from the Apache Software Foundation. Upon hitting an nonexistent JSP file, too much information is presented by the server as part of the error message. This information may be useful to a would be attacker in conducting further attacks.

- **Apache Tomcat Snoop Servlet Information Disclosure Vulnerability**

A vulnerability exists in the snoop servlet portion of the Tomcat package, version 3.1, from the Apache Software Foundation. Upon hitting an nonexistent

file with the .snp extension, too much information is presented by the server as part of the error message. This information may be useful to a would be attacker in conducting further attacks. This information includes full paths, OS information, and other information that may be sensitive.

- **Apache Tomcat Simultaneous Directory Listing Denial Of Service Vulnerability**

A remote denial of service vulnerability affects Apache Tomcat. This issue is due to a failure of the application to efficiently handle multiple directory listing requests.

Once this issue has been triggered, the application fails to serve further requests to legitimate users until the Tomcat processes have been restarted.

An attacker may leverage this issue to trigger a denial of service condition in the affected software.

- **Microsoft Windows Graphics Rendering Engine WMF/EMF Format Code Execution Vulnerability**

Microsoft Windows WMF/EMF graphics rendering engine is affected by a remote code execution vulnerability.

The problem presents itself when a user views a malicious WMF or EMF formatted file causing the affected engine to attempt to parse it. Exploitation of this issue can trigger an integer overflow that may facilitate heap memory corruption and arbitrary code execution.

Any code execution that occurs will be with SYSTEM privileges due to the nature of the affected engine. Successful exploitation can facilitate a remote compromise or local privilege escalation.

- **Microsoft Windows Graphics Rendering Engine WMF Format Code Execution Vulnerability**

Microsoft Windows WMF graphics rendering engine is affected by a remote code execution vulnerability.

The problem presents itself when a user views a malicious WMF formatted file, triggering the vulnerability when the engine attempts to parse the file. A malicious file can cause an integer overflow that may facilitate heap memory corruption and arbitrary code execution.

Any code execution that occurs will be with SYSTEM privileges due to the nature of the affected engine. Successful exploitation can facilitate a remote compromise or local privilege escalation.

- **Cisco IPSec Unspecified IKE Traffic Denial Of Service Vulnerabilities**

Various Cisco IOS, PIX Firewall, Firewall Services Module (FWSM), VPN 3000 Series Concentrator, and MDS Series SanOS releases are prone to denial of

service attacks. These issues are due to security flaws in Cisco's IPSec implementation. The vulnerabilities may be triggered by malformed IKE traffic.

Successful attacks will cause most affected devices to restart. For Cisco MDS Series devices, this is limited to causing the IKE process to restart.

- **Apache Jakarta-Tomcat /admin Context Vulnerability**

The Tomcat package, from the Apache Software Foundation, contains a vulnerability that could cause the disclosure of information that could lead to the compromise of the machine running Tomcat. By default, Tomcat contains a mounted context, /admin, that contains servlets that can be used to add and delete contexts, or view context information on the Tomcat server. By adding the root directory (/) as a context, it is possible to view files readable by the account Tomcat is running as. If Tomcat is running as root, all files on the filesystem may be accessed. This can in turn lead to the retrieval of vital information that may be used to gain access to the machine. There is no access control present to prevent unauthorized access to the /admin context. As such, any remote user can potentially exploit this vulnerability.

- **Microsoft Internet Explorer Dialog Manipulation Vulnerability**

Internet Explorer is prone to a remote code execution vulnerability through manipulation of custom dialog boxes. Keystrokes entered while one of these dialogs is displayed may be buffered and passed to a download dialog, allowing attacker-supplied code to be executed.

- **Microsoft Internet Explorer HTTPS Proxy Information Disclosure Vulnerability**

Microsoft Internet Explorer is prone to an information disclosure vulnerability when using an authenticating proxy server for HTTPS communications. Exploitation of this issue could result in an attacker gaining a user's authentication credentials.

This issue only exists when the authenticating proxy uses Basic Authentication.

- **Microsoft Windows Asynchronous Procedure Call Local Privilege Escalation Vulnerability**

Microsoft Windows is susceptible to a local privilege escalation vulnerability. This issue is due to a flaw in the Asynchronous Procedure Calls implementation in Microsoft Windows.

This issue allows local attackers to gain elevated privileges, facilitating the complete compromise of affected computers.

- **Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability**

Microsoft Internet Explorer is prone to a memory corruption vulnerability that is related to the instantiation of COM objects.

COM objects may corrupt system memory and facilitate arbitrary code execution in the context of the currently logged in user on the affected computer.

- **Apache Web Server DoS Vulnerability**

Apache Web Server 1.2 and previous versions, are subject to a denial of service. Requesting a malformed GET request composed of an unusually large number of '/', will cause the CPU utilization to spike. A restart of the service is required in order to gain normal functionality.

- **NCSA/Apache httpd ScriptAlias Source Retrieval Vulnerability**

NSCA httpd prior to and including 1.5 and Apache Web Server prior to 1.0 contain a bug in the ScriptAlias function that allows remote users to view the source of CGI programs on the web server, if a ScriptAlias directory is defined under DocumentRoot. A full listing of the CGI-BIN directory can be obtained if indexing is turned on, as well. This is accomplished by adding multiple forward slashes in the URL (see exploit). The web server fails to recognize that a ScriptAlias directory is actually redirected to a CGI directory when this syntax is used, and returns the text of the script instead of properly executing it. This may allow an attacker to audit scripts for vulnerabilities, retrieve proprietary information, etc.

- **PKCS #1 Version 1.5 Session Key Retrieval Vulnerability**

The data encryption techniques described in RSA's PKCS #1 standard are used in many protocols which rely on, at least in part, the security provided by public-key cryptography systems.

Several protocols which implement the digital enveloping method described in version 1.5 of the PKCS #1 standard are susceptible to an adaptive ciphertext attack which may allow the recovery of session keys, thus compromising the integrity of the data transmitting during that session.

By capturing and logging the packets transmitted between a client and a server, an opponent could make use of a captured encrypted session key to launch a Bleichenbacher attack together with a simple timing attack. If the session key is successfully decrypted, the saved packets can easily be decrypted in a uniform manner.

Interactive key establishment protocols, such as SSH or SSL, are generally significantly more susceptible to successful attacks.

- **Apache Artificially Long Slash Path Directory Listing Vulnerability**

Apache HTTPD is the Apache Web Server, freely distributed and actively maintained by the Apache Software Foundation. It is a freely available and widely used software package, included with various implementations of the UNIX Operating System, and can be used on Microsoft Operating Systems.

A problem in the package could allow directory indexing, and path discovery. In a default configuration, Apache enables mod_dir, mod_autoindex, and mod_negotiation. However, by placing a custom crafted request to the Apache server consisting of a long path name created artificially by using numerous slashes, this can cause these modules to misbehave, making it possible to escape the error page, and gain a listing of the directory contents.

This vulnerability makes it possible for a malicious remote user to launch an information gathering attack, which could potentially result in compromise of the system. Additionally, this vulnerability affects all releases of Apache previous to 1.3.19.

- **Apache Tomcat 3.0 Directory Traversal Vulnerability**

Apache Tomcat in a Windows NT environment could be led to traverse the normal directory structure and return requested files from outside of the document root.

By including '/../' sequences along with specially chosen characters in requested URLs, a remote user can obtain read access to directories and files outside of the document root, potentially compromising the privacy of user data and/or obtaining information which could be used to further compromise the host.

Multiple Vendor URL JSP Request Source Code Disclosure Vulnerability

BEA Systems WebLogic Server is an enterprise level web and wireless application server.

Tomcat can be used together with the Apache web server or a stand alone server for Java Servlets and Java Pages. Tomcat ships with a built in web server.

Tomcat and WebLogic's inbuilt webserver will return the source code of JSP files when an HTTP request contains URL encoded replacements for characters in the filename.

If successfully exploited this vulnerability could lead to the disclosure of sensitive information contained within JSP pages. This information may assist in further attacks against the host.

- **Multiple Vendor TCP Initial Sequence Number Statistical Vulnerability**

Over the past several years, a variety of attacks against TCP initial sequence number (ISN) generation have been discussed.

A vulnerability exists in some TCP/IP stack implementations that use random increments for initial sequence numbers. Such implementations are vulnerable to statistical attack, which could allow an attacker to predict, within a reasonable range, sequence numbers of future and existing connections.

By predicting a sequence number, several attacks could be performed; an attacker could disrupt or hijack existing connections, or spoof future connections.

- **Apache Possible Directory Index Disclosure Vulnerability**

A possible vulnerability exists in Apache that could cause directory contents to be disclosed when directory indexing is enabled, despite the presence of an 'index.html' file.

The problem is likely the result of an error in multiview functionality provided as part of Apache's content negotiation support. Exploitation of this problem may lead to the disclosure of sensitive information to attackers.

- **Apache Server Address Disclosure Vulnerability**

A vulnerability has been discovered in Apache web server that may result in the disclosure of the server's address.

The problem occurs when a HTTP request containing the URI of a directory is submitted to the server. If the URI does not contain a trailing '/' character, the server returns a 3xx redirection error code indicating that further action must be taken in order to fulfill the request. When this occurs, a 'Location' response-header containing the address of the server is returned as part of the response.

In a situation where the request is redirected to the server behind a firewall, this could lead to the disclosure of the server's internal network address.

- **Apache Mod ReWrite Rules Bypassing Image Linking Vulnerability**

Apache is a freely available, widely used web server distributed and maintained by the Apache Server Project.

It is possible to bypass mod_rewrite rules if the rules are constructed in a certain way, such as:

RewriteCond %{HTTP_REFERER} !>http://www\.yoursite\.com.*$

RewriteRule >/images/.* - [G]

This does not filter requests for the //images directory, and could allow a remote site to link images, resulting in increased hosting costs, and potentially a denial of service.

- **Jakarta Tomcat Error Message Information Disclosure Vulnerability**

When a malformed request is made for a Java Server Page the server displays an error page. The error page contains potentially sensitive information, along with the absolute path of the JSP file on the webserver, which may aid in further attacks.

Jakarta Tomcat can be configured to display an alternate error file. By default it is not.

- **Apache mod_usertrack Predictable ID Generation Vulnerability**

Apache is a popular open-source HTTP server in wide use across the Internet. Apache ships with a module called 'mod_usertrack'. This module contains code to generate unique identifiers for individual web sessions and requests.

The session IDs that are generated are not random. They are generated using the IP address of the client, the system time and the server process ID. These IDs are not meant to be used for authentication purposes.

Any applications that rely on these IDs for authentication may be vulnerable to ID prediction attacks.

It should be noted that this is not a vulnerability in Apache. This is only a vulnerability when an application uses these IDs to track authenticated users.

- **Cisco Access Control List Fragment Keyword Ignored Vulnerability**

IOS is the Cisco Internet Operating System, distributed with and used on various Cisco network hardware.

A vulnerability in IOS on the 12000 series Cisco routers could make it possible for a remote user to send unauthorized traffic to a protected network. IOS does not filter packet fragments, even when the 'fragment' keyword is included in an ACL rule.

This vulnerability may result in attackers or users bypassing security policy.

- **Apache Split-Logfile File Append Vulnerability**

Split-logfiles in Apache webserver allow separate log files to be created for each individual host name.

A problem exists in the implementation of the split-logfile functionality which may allow attacker-supplied data to be appended to files with the .log extension.

A HTTP request with a Host: header that starts with a “/” will cause an error message to be displayed, but will also still append the entry to the appropriate access file. This can be exploited to cause attacker-supplied data to be appended to an arbitrary .log file if the Host: header is specially crafted.

Red Hat Secure Web Server 3.2 is also affected by this issue.

- **Apache Non-Existent Log Directory Denial Of Service Vulnerability**

Under certain circumstances Apache is prone to exhibit unusual behavior, leading to a potential local denial of service attack.

When Apache is stopped, it will attempt to reload its configuration file and then proceed to shutdown. Certain problems occur if an entry for a previously existing log directory is still present in the configuration file. Apache will not be able to restart if it tries to access a previously existing log directory that has been since removed.

It should be noted that this is only really an issue if the intended setup is that unprivileged local users are able to remove directories.

This issue is believed to affect Apache running on Unix and Linux variants.

- **Apache HTTP Request Unexpected Behavior Vulnerability**

Under some circumstances, Apache may yield unexpected results for specific HTTP requests. This may be related to the BID 3569 or 3009, available at the following locations:

http://www.securityfocus.com/bid/3569

http://www.securityfocus.com/bid/3009

While further details are not available at this time, HP has released a patch resolving this issue for HP Secure OS software for Linux Release 1.0.

- **Apache 2 for Windows php.exe Path Disclosure Vulnerability**

Apache is a powerful, widely used web server available for most operating systems, including Linux, Windows and many other Unix like systems. Apache 2 is currently in development, and beta versions have been made available to the public.

A path disclosure vulnerability exists in the default configuration of some beta releases of Apache 2. If PHP is also installed with default values, it is possible to submit a malicious request to the web server such that the full path of the PHP interpreter is disclosed.

A url of the form http://host/file.php/123 will result in an error message, including in part the path of the file php.exe.

- **Apache 2 for Windows OPTIONS request Path Disclosure Vulnerability**

Apache is a powerful, widely used web server available for most operating systems, including Linux, Windows and many other Unix like systems. Apache 2 is currently in development, and beta versions have been made available to the public.

A path disclosure vulnerability exists in the default configuration of some beta releases of Apache 2. If an HTTP OPTIONS request is made to the vulnerable server, the content returned will include the full path of the php.exe script handler.

SecurityFocus has not been able to reproduce this vulnerability. It is possible that this issue is the result of a specific configuration.

- **Cisco Malformed SNMP Message Denial of Service Vulnerabilities**

Cisco products contain multiple vulnerabilities in handling of SNMP requests and traps. A general report for multiple vendors was initially published on February 12 (Bugtraq IDs 4088 and 4089), however more information is now

available and a separate Bugtraq ID has been allocated for the Cisco Operating Systems and Appliances vulnerabilities.

It is reportedly possible for a remote attacker to create a denial of service condition by transmitting a malformed SNMP request to a vulnerable Cisco Operating System or Appliance. The affected device may reset, or require a manual reset to regain functionality.

- **Apache Double-Reverse Lookup Log Entry Spoofing Vulnerability**

Apache is a freely available webserver for Unix and Linux variants, as well as Microsoft operating systems.

Under some circumstances, Apache may log invalid hostname information. If a double-reverse DNS lookup is performed but fails, then an invalid hostname may appear in the logs. For example, this may occur if the hostname does not properly resolve to the IP address in the double-reverse DNS lookup.

A remote attacker may deliberately exploit this issue to cause spoofed information to be logged by the webserver.

- **Apache PrintEnv/Test_CGI Script Injection Vulnerability**

Printenv and test_cgi are default scripts that ship with Apache webserver. Apache releases prior to 1.3.12 ship with versions of these scripts that do not properly escape HTML tags. As a result, it may be possible for an attacker to include arbitrary script code in values that will be outputted to webpages by the vulnerable CGI scripts.

The vendor addressed this issue by changing the content-type sent by these scripts to a MIME type of text/plain. However, it should be noted that some web browsers, in particular Microsoft Internet Explorer, do not correctly handle this MIME type, causing anything that looks like HTML tags in a webpage to be interpreted as such. The consequence is that it is still possible to cause script code to be executed by some browsers.

- **Apache Error Message Cross-Site Scripting Vulnerability**

A number of Apache core files and modules do not properly escape HTML tags from error messages that are generated and displayed in webpages. If an attacker can cause arbitrary data to be displayed in error output then it is also possible to inject malicious script code. The attacker-supplied script code will be executed in the browser of a user who views the webpage containing the error message.

For example, the attacker might construct a malicious link which causes an error page containing script code to be generated when the link is visited. The attacker may then send the malicious link in a HTML e-mail to an arbitrary user. When the user visits the link, the script code will be executed in the context of the page they are visiting.

- **Cisco IOS 12.1 Large TCP Scan Denial of Service Vulnerability**

IOS is the Internet Operating System, used on Cisco routers. It is distributed and maintained by Cisco.

Some versions of IOS may suffer from a denial of service condition when large port scans are performed through the vulnerable router. Reportedly, scanning a single host on all 65535 possible ports or scanning a class C network block for a single port are sufficient to exploit this vulnerability.

This vulnerability has been reported to exist on a Cisco 2611 router running IOS 12.1(6.5). Cisco has reported that they are unable to reproduce this problem. It is possible that this issue is the result of a configuration error or site specific conditions.

- **Cisco Malformed HSRP Traffic Denial of Service Vulnerability**

IOS is the Internet Operating System, used on Cisco routers. It is distributed and maintained by Cisco. Hot Standby Routing Protocol (HSRP) is a protocol used to allow multiple routers to dynamically act as backups in the event of router failure. HSRP traffic takes place over UDP port 1985.

A vulnerability has been reported with some Cisco products. If malformed HSRP traffic is received when HSRP support is not enabled, vulnerable products may reach high CPU utilization. Under these conditions, the router may fail to respond to additional network traffic, resulting in degraded performance and a denial of service condition.

- **Cisco Spoofed HSRP Loopback Denial Of Service Vulnerability**

IOS is the Internet Operating System, used on Cisco routers. It is distributed and maintained by Cisco. Hot Standby Routing Protocol (HSRP) is a protocol used to allow multiple routers to dynamically act as backups in the event of router failure. HSRP traffic takes place over UDP port 1985.

A vulnerability has been reported in some versions of IOS. It may be possible for maliciously constructed HSRP traffic to create a loop condition, resulting in a denial of service attack.

It has been reported possible to cause this condition in version 12.1 of IOS. Other versions of IOS may share this vulnerability, this has not however been confirmed. This issue has been assigned Cisco Bug ID CSCdu38323.

- **Cisco View-based Access Control MIB SNMP Walk Read-Write Password Revealing Vulnerability**

Cisco IOS and CatOS are the network firmware developed and maintained by Cisco.

The problem involves the design of the View Access Control MIB (VACM) used by Cisco firmware. Under some circumstances, it may be possible for a remote

user to gain access to the Read-Write password. This could allow an attacker to change configuration settings on the device.

- **Cisco uBR7200 / uBR7100 Universal Broadband Routers DOCSIS MIC Bypass Vulnerability**

A vulnerability has been announced which affects Cisco uBR7200 series and uBR7100 series Universal Broadband Routers under some versions of IOS.

Invalid DOCSIS files without an MIC signature may be accepted by a vulnerable router, even if MIC signatures are required. Exploitation of this vulnerability may allow arbitrary configuration files to be accepted by the network.

- **Apache Tomcat DOS Device Name Cross Site Scripting Vulnerability**

A vulnerability has been reported for Apache Tomcat 4.0.3 on a Microsoft Windows platform. Reportedly, it is possible for an attacker to launch a cross site scripting attack.

When making a request for a DOS device file name, Tomcat will throw an exception and respond with an error message. It is also possible for information to be appended to the DOS device when making a request.

- **Cisco Access List Vulnerability**

A vulnerability in Cisco access lists allows some packets to be erroneously routed which one would expect to be filtered by the access list and vice-versa. This vulnerability can allow unauthorized traffic to pass through the gateway and can block authorized traffic.

If a Cisco router is configured to use extended IP access lists for traffic filtering on an MCI, SCI, cBus or cBusII interface, and the IP route cache is enabled, and the “established” keyword is used in the access list, then the access list can be improperly evaluated. This can permit packets which should be filtered and filter packets which should be permitted.

- **Apache HTDigest Insecure Temporary File Vulnerability**

Apache creates temporary files insecurely for htdigest. As a result, it is possible for local attackers to read or corrupt the Apache password file. If the attacker can write custom-data to the password file, it may be possible to gain unauthorized access to resources protected by htpasswd. Alternatively, an attacker could reportedly read the password file and gain unauthorized access to credentials.

- **Cisco AS5350 Universal Gateway Portscan Denial Of Service Vulnerability**

The Cisco AS5350 Universal Gateway is reported to be prone to a denial of service condition. It is possible to cause this condition by portscanning a vulnerable device.

This issue was reported for Cisco AS5350 devices running Cisco IOS release 12.2(11)T. Other firmware and devices may also be affected.

There are conflicting reports regarding the existence of this vulnerability. One source states that this condition reportedly does not occur if there are no Access Control Lists (ACL) applied on the device and also mentions that this may be related to a known SSH bug. Other sources have indicated that the issue may be related to a configuration problem.

- **Apache mod_php File Descriptor Leakage Vulnerability**

A vulnerability has been discovered in the mod_php module available for Apache web servers that may, under some circumstances, leak file descriptor information. By exploiting this vulnerability it may be possible for a remote attacker to reuse file descriptors used by the httpd daemon, effectively taking control of TCP port 80.

Exploitation of this issue may allow an attacker to bind a malicious server in place of Apache httpd server.

It should be noted that this issue is exploitable only if the 'safe_mode' PHP option is disabled.

- **Apache/Tomcat Mod_JK Chunked Encoding Denial Of Service Vulnerability**

Apache Webserver and Tomcat are HTTP servers maintained and distributed by the Apache project. Apache Webserver and Tomcat are available for the Unix, Linux, and Microsoft Windows platforms.

It has been reported that a denial of service exists in Apache Webserver and Tomcat when mod_jk is used. Due to design problems in the module, a user submitting malicious requests to the Apache Webserver may cause desynchronization between Apache and Tomcat. This could be done through malicious chunked encoding requests.

- **Cisco OSM Line Cards Denial Of Service Vulnerability**

A vulnerability has been discovered in OSM Line Cards when installed in various Cisco devices. Cisco has reported that a denial of service may occur when processing an irregularly constructed network packet. Exploitation of this issue will cause the Cisco device to no longer forward legitimate packets.

Precise technical details regarding this vulnerability are not yet known. This BID will be updated as further information becomes available.

- **Multiple Vendor SSH2 Implementation Incorrect Field Length Vulnerabilities**

A vulnerability with incorrect lengths of fields in SSH packets have been reported for multiple products that use the SSH2 for secure communications.

The vulnerabilities have been reported to affect initialization, key exchange, and negotiation phases of SSH communications. An attacker may exploit these vulnerabilities to perform denial of service attacks against vulnerable systems and possibly to execute malicious, attacker-supplied code.

Further details about the vulnerability are currently unknown. This BID will be updated as more information becomes available. This vulnerability was originally described in BugTraq ID 6397.

- **Multiple Vendor SSH2 Implementation Empty Elements / Multiple Separator Vulnerabilities**

A vulnerability has been reported for multiple SSH2 vendors. The vulnerability is a result of SSH2 packets containing empty elements/multiple separators.

The vulnerability has been reported to affect initialization, key exchange, and negotiation phases of SSH communications. An attacker may exploit this vulnerability to perform denial of service attacks against vulnerable systems and possibly to execute malicious, attacker-supplied code.

Further details about this vulnerability are currently unknown. This BID will be updated as more information becomes available. This vulnerability was originally described in BugTraq ID 6397.

- **Multiple Vendor SSH2 Implementation Null Character Handling Vulnerabilities**

Multiple vendor SSH2 implementations are reported to be prone to issues related to the handling of null characters in strings. These issues may be used to cause unpredictable behavior to occur, such as a denial of service or memory corruption. It is reportedly possible to trigger these conditions prior to authentication.

These conditions were discovered during tests of the initialization, key exchange, and negotiation phases (KEX, KEXINIT) of a SSH2 transaction between client and server. These issues are known to affect various client and server implementations of the protocol.

Further details about this vulnerability are currently unknown. This BID will be updated as more information becomes available. This vulnerability was originally described in BugTraq ID 6397.

- **Cisco PIX and CBAC Fragmentation Attack**

Both the Cisco PIX Firewall software as the Context-based Access Control (CBAC) feature of Cisco's IOS Firewall Feature Set do not properly check non-initial fragmented IP packets. Although the non-initial fragmented IP packets might belong to session which would normally be blocked, they are forwarded to the destination host. This may lead to a denial of services (DOS) attack due to the exhaustion of resources required to keep track of the fragmented IP packets.

The problem can be fixed by keeping track of the sessions that fragmented IP packets belong to and by blocking non-initial fragmented IP packets for which no initial packet has been seen.

The DOS attack can easily be carried out by publicly available tools.

- **Cisco Aironet AP1x00 Malformed HTTP GET Denial Of Service Vulnerability**

Cisco Aironet AP1x00 series devices are prone to a denial of service vulnerability upon receipt of a malformed HTTP GET request. Such a request will cause the device to reload.

- **Cisco Aironet Telnet Service User Account Enumeration Weakness**

An information leak has been reported in Cisco Aironet Access Points when the telnet service has been enabled. This may allow a remote attacker to gain potentially sensitive information.

- **Apache htpasswd Password Entropy Weakness**

A weakness has been discovered in the way that the Apache htpasswd utility generates salts. Specifically, the salt is generated based of the current system time. As a result, salts generated within the same second will be identical. This may pose a security weakness if the server were implementing the use of default passwords and an attacker were capable of disclosing the contents of htpasswd.

- **Apache2 MOD_CGI STDERR Denial Of Service Vulnerability**

Apache2 has been reported prone to a denial-of-service vulnerability. The issue has been reported to present itself when a CGI script outputs excessive data to STDERR. If this condition occurs the execution of the script will reportedly pause indefinitely due to a locked write() call in mod_cgi. Because Apache2 is waiting for further input from the malicious CGI application, the httpd process may hang. When the maximum connection limit is reached, Apache will no longer service requests, effectively denying service to legitimate users.

- **Apache Tomcat Non-HTTP Request Denial Of Service Vulnerability**

Apache Tomcat 4 has been reported prone to a remotely triggered denial of service vulnerability when handling undisclosed non-HTTP request types.

It has been reported that when certain specific non-HTTP request types are handled by the Tomcat HTTP connector the Tomcat server will reject subsequent requests on the affected port until the service is restarted.

- **OpenSSL ASN.1 Large Recursion Remote Denial Of Service Vulnerability**

A problem has been identified in OpenSSL when handling specific types of ASN.1 requests. This may result in remote attackers creating a denial of service condition.

This issue is also known to affect numerous Cisco products. It is possible that other vendors will also be acknowledging this issue and providing fixes.

- **Apache mod_php Module File Descriptor Leakage Vulnerability**

It has been reported that Apache mod_php module may be prone to a vulnerability that may allow a local attacker to gain access to privileged file descriptors. This may result in the attacker posing as a legitimate server and possibly stealing/manipulating sensitive information.

- **Multiple Vendor H.323 Protocol Implementation Vulnerabilities**

It has been reported that multiple vendor implementations of the H.323 protocol contain various vulnerabilities. These vulnerabilities may range from simple denial of service to potential arbitrary code execution.

- **Apache mod_perl Module File Descriptor Leakage Vulnerability**

A vulnerability has been reported to exist in the Apache mod_perl module that may allow local attackers to gain access to privileged file descriptors. This issue could be exploited by an attacker to hijack a vulnerable server daemon. Other attacks are also possible.

It has been reported that multiple file descriptors, are leaked to the mod_perl module and any processes it creates. This allows for Perl scripts and any processes they spawn to access the privileged I/O streams.

It should be noted that this issue appears to be distinct from the vulnerability described in BID 7255 (and patched in Apache 2.0.45). Versions later than Apache 2.0.45 reportedly still leak descriptors.

- **Apache mod_digest Client-Supplied Nonce Verification Vulnerability**

Patches have been released for the Apache mod_digest module to include digest replay protection. The module reportedly did not adequately verify client-supplied nonces against the server issued nonce. This could permit a remote attacker to replay the response of another website or section of the same website under some circumstances.

It should be noted that this issue does not exist in mod_auth_digest module.

- **Apache mod_php Global Variables Information Disclosure Weakness**

It has been reported that Apache mod_php may be prone to a weakness that may allow remote attackers to disclose sensitive information via influencing global variables. This issue may lead to other vulnerabilities that result from setting register_globals to on, due to an attacker's ability to influence global variables. An attacker may also be able to disclose sensitive information in order to gain unauthorized access.

- **Multiple Vendor HTTP Response Splitting Vulnerability**

A paper (Divide and Conquer - HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics) was released to describe various attacks that target web users through web application, browser, web/application server and proxy implementations. These attacks are described under the general category of HTTP Response Splitting and involve abusing various input validation flaws in these implementations to split HTTP responses into multiple parts in such a way that response data may be misrepresented to client users.

Exploitation would occur by injecting variations of CR/LF sequences into parts of HTTP response headers that the attacker may control or influence. The general consequences of exploitation are that an attacker may misrepresent web content to the client, potentially enticing the user to trust the content and take actions based on this false trust.

While the various implementations listed in the paper contribute to these attacks, this issue will most likely be exposed through web applications that do not properly account for CR/LF sequences when accepting user-supplied input that may be returned in server responses.

This vulnerability could also aid in exploitation of cross-site scripting vulnerabilities.

- **Multiple Vendor SNMP World Writeable Community Vulnerability**

In a number of network devices/operating systems there exist default communities which are world writeable. By being world writeable, they allow remote users to configure properties of the device/OS without any authorization other than knowledge of the community name.

Some of the common default communities/vendors are:

- public (ascend,cisco,bay networks (nortel),microsoft,sun,3com, aix)
- private (cisco,bay networks (nortel),microsoft,3com, brocade, aix, netapp)
- write (ascend, very common)
- all private (sun)
- monitor (3com)
- manager (3com)
- security (3com)
- OrigEquipMfr (brocade)
- Secret C0de (brocade)
- admin
- default

- password
- tivoli
- openview
- community
- snmp
- snmpd
- system (aix, others)
- the name of the router (ie, 'gate')

The attacks can be things such as routing table manipulation and arp cache corruption, which can lead to further compromise.

- **Apache HTAccess LIMIT Directive Bypass Configuration Error Weakness**

LIMIT directives are commonly used in htaccess files to restrict HTTP methods that are available for a particular resource. However it has been reported that if the requested resource is served by an Apache module and not by Apache Server itself, LIMIT restrictions may not apply. Additionally, CGI/Script resources that do not sufficiently check the calling method may potentially be invoked with methods not listed in the LIMIT clause to evade LIMIT restrictions.

- **Apache Connection Blocking Denial Of Service Vulnerability**

Apache is prone to an issue that may permit remote attackers to cause a denial of service issue via a listening socket on a rarely accessed port. This will reportedly block out new connections to the server until another connection on the rarely accessed socket is initiated.

The functionality that exposes this issue is reportedly enabled by default on all platforms except Windows.

Security Update 26

Symantec NetRecon 3.6 Security Update 26 (SU26) detects and reports 52 new vulnerabilities.

New vulnerability detection

- **Multiple Vendor Telnet Client Remote Information Disclosure Vulnerability**

Telnet clients provided by multiple vendors are susceptible to a remote information disclosure vulnerability.

Any information stored in the environment of clients utilizing the affected telnet application is available for attackers to retrieve. The contents of the environment variables may be sensitive in nature, allowing attackers to gain information that may aid them in further system compromise.

- **Microsoft Internet Explorer PNG Image Rendering Buffer Overflow Vulnerability**

Microsoft Internet Explorer is prone to a buffer overflow vulnerability. This issue exists in the PNG image rendering library used by the browser.

Successful exploitation will result in execution of arbitrary code in the context of the currently logged in user.

This issue is present in the PNG image rendering library, so it is possible that other applications that use the library are affected. This is not confirmed and Symantec is not aware of any such applications.

- **Microsoft Incoming SMB Packet Validation Remote Buffer Overflow Vulnerability**

Microsoft SMB is susceptible to a remote buffer overflow vulnerability. This issue is due to a failure of the application to properly bounds check user-supplied data prior to copying it to an insufficiently sized memory buffer.

Remote attackers may exploit this vulnerability to execute arbitrary machine code in the context of the kernel containing the vulnerable code. Microsoft has stated that other attack vectors may exist, in the form of passing malicious parameters to the affected component, either locally or remotely.

Failed exploit attempts will likely crash the affected computer, denying service to legitimate users.

- **Microsoft Internet Explorer XML Redirect Information Disclosure Vulnerability**

Microsoft Internet Explorer is prone to an information disclosure vulnerability. Specifically, it may be possible for remote users to read XML data from an affected computer via a malicious Web page.

This issue is a variant of BID 5560. This variant was not addressed with the release of MS02-047. Microsoft has released a new security bulletin to provide fixes for this variant. Microsoft has stated that Windows Server 2003 with the Enhanced Security Configuration enabled is not affected.

- **Microsoft Internet Explorer Unspecified DigWebX ActiveX Control Vulnerability**

Microsoft Internet Explorer is prone to an unspecified vulnerability in the DigWebX ActiveX control.

The vendor has not released any further information about this vulnerability other than to state the "kill bit" has been set on unsupported versions of the control.

- **Microsoft Internet Explorer Unspecified GIF And BMP Denial Of Service Vulnerability**

Microsoft Internet Explorer is prone to a denial of service vulnerability when rendering malformed GIF and BMP images. Malformed images for other file formats may also cause a similar condition, though the vendor has not provided any further information.

The vendor has not released any further information about this issue other than to state that it is addressed by the Cumulative Security Update For Internet Explorer.

- **Microsoft Agent Trusted Content Spoofing Vulnerability**

Microsoft Agent is prone to a vulnerability that could allow a malicious Web site to spoof trusted content. This could result in a user downloading and executing malicious files thinking they are safe.

- **Microsoft Windows Web Client Service Remote Code Execution Vulnerability**

Microsoft Windows Web Client Service is affected by a remote code execution vulnerability. This is due to a buffer overflow in the affected component.

A remote authenticated attacker can exploit this issue by sending a malformed message to the Web Client Service. This can lead to arbitrary code execution resulting in privilege escalation.

An attacker may also exploit this issue through another application that passes data to the vulnerable component.

Web Client Service is disabled on Windows Server 2003 by default.

- **Microsoft Outlook Express NNTP Response Parsing Buffer Overflow Vulnerability**

Microsoft Outlook Express is prone to a buffer overflow when parsing NNTP responses. Successful exploitation could allow arbitrary code execution in the context of the user running the application.

- **Microsoft Exchange Server Outlook Web Access HTML Injection Vulnerability**

Outlook Web Access is prone to an HTML injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input.

An attacker may leverage this issue to have arbitrary script code executed in the affected application of an unsuspecting user in the context of the affected user.

This issue is reported to affect Outlook Web Access for Exchange Server 5.5.

- **Microsoft Internet Explorer Javaprxy.DLL COM Object Instantiation Heap Overflow Vulnerability**

Microsoft Internet Explorer is prone to a heap-based buffer overflow vulnerability. The vulnerability is exposed when the 'javaprxy.dll' COM object is instantiated by a malicious Web page.

This issue may potentially be exploited to execute arbitrary code in the context of the client.

- **Microsoft Windows Color Management Module ICC Profile Buffer Overflow Vulnerability**

Microsoft Windows is prone to a buffer overflow vulnerability in the Color Management Module. The issue is due to a boundary condition error related to the parsing of ICC (International Color Consortium) Profile tags in various supported image and document formats.

ICC Profile data may possibly be embedded in various file formats, including JPEG, GIF, EXIF, TIFF, PNG, PICT, PDF, PostScript, SVG, JDF, and CSS3. Some of these formats may not provide an attack vector, especially if Microsoft does not provide native support or does not call the vulnerable functionality when handling certain formats.

Successful exploitation may result in execution of arbitrary code in the context of the currently logged in user. This vulnerability could be exploited through a Web site that hosts a malicious document, by previewing or opening malicious content in email, or through other means that will allow an attacker to send the victim a malicious document.

There is also a risk that other Microsoft or third-party applications that rely on the affected functionality may be vulnerable. A number of third-party applications may ship with vulnerable libraries, so may remain vulnerable despite having applied the Microsoft patch. Symantec is not aware of any such vendors at the time of writing.

- **Microsoft Windows Logon Process Remote Buffer Overflow Vulnerability**

Microsoft Windows logon process "winlogon" has been reported to be prone to a remote buffer overflow vulnerability. The issue is reported to exist when the vulnerable host is a member of an Active Directory domain. When processing logon information, the windows logon process will read data from the Active Directory. This read call does not sufficiently perform bounds checking on received data before said data is copied into a reserved buffer in process memory.

Supplied data that exceeds the size of the allocated buffer in Windows logon process memory will overrun its bounds, this will result in the corruption of memory that is adjacent to the affected buffer.

- **Microsoft Windows ASN.1 Library Bit String Processing Variant Heap Corruption Vulnerability**

Microsoft ASN.1 handling library has been reported prone to a heap corruption vulnerability. The issue presents itself in the ASN.1 bit string decoding routines, specifically the BERDecBitString() function. The issue manifests when the affected function attempts to process a constructed bit string that contain another nested constructed bit string.

This vulnerability is exposed in a number of security related operating system components, including Kerberos (via UDP port 88), Microsoft IIS with SSL support enabled and NTLMv2 authentication (via TCP ports 135, 139 and 445). Other components may also be affected, though a comprehensive list is not available at this time. Client applications, which use the library, will be affected, including LSASS.EXE and CRYPT32.DLL (and any application that relies on CRYPT32.DLL). The vulnerable library is used frequently in components that handle certificates such as Internet Explorer and Outlook. Handling of signed ActiveX components could also present an exposure.

It should be noted that because ASN.1 data will likely be encoded, for example Kerberos, SSL, IPSec or Base64 encoded, the malicious integer values may be obfuscated and as a result not easily detectable.

Issues related to this vulnerability were originally covered in BID 9626 and 9743, further information has been made available which identifies that this is a distinct vulnerability in the library and so this specific issue has been assigned an individual BID.

- **Microsoft Windows Kernel Unspecified Remote Desktop Protocol Denial Of Service Vulnerability**

A remote denial of service vulnerability has been reported in the kernel for Microsoft Windows. The vendor has confirmed that this vulnerability permits remote attackers to crash affected computers. This issue is due to a failure of the application to properly handle malformed Remote Desktop requests.

- **Microsoft Internet Explorer JPEG Image Rendering Unspecified Buffer Overflow Vulnerability**

Microsoft Internet Explorer is prone to a buffer overflow vulnerability in the JPEG image rendering library used by the browser. This issue is due to a failure of the application to properly bounds check input data prior to copying it to a fixed size memory buffer.

This issue was identified by creating random input for the browser, and has not been researched further at this time. This BID will be updated as further information is disclosed.

Successful exploitation may result in execution of arbitrary code in the context of the user executing the affected browser.

- **Microsoft Internet Explorer JPEG Image Rendering CMP Fencepost Denial Of Service Vulnerability**

Microsoft Internet Explorer is prone to an unspecified denial of service vulnerability in the JPEG image rendering library used by the browser. This issue is reportedly similar to the one described in BID 14282.

This issue was identified by creating random input for the browser, and has not been researched further at this time. This BID will be updated as further information is disclosed.

Successful exploitation results in crashing the affected Web browser. It may be possible that execution of arbitrary code may also be achieved, but this has not been confirmed.

- **Microsoft Internet Explorer JPEG Image Rendering Memory Consumption Denial Of Service Vulnerability**

Microsoft Internet Explorer is prone to an unspecified denial of service vulnerability in the JPEG image rendering library used by the browser.

This issue was identified by creating random input for the browser, and has not been researched further at this time. This BID will be updated as further information is disclosed.

Successful exploitation results in crashing the affected Web browser by consuming excessive memory.

- **Microsoft Internet Explorer JPEG Image Rendering Unspecified Denial Of Service Vulnerability**

Microsoft Internet Explorer is prone to an unspecified denial of service vulnerability in the JPEG image rendering library used by the browser.

This issue was identified by creating random input for the browser, and has not been researched further at this time. This BID will be updated as further information is disclosed.

Successful exploitation results in crashing the affected Web browser. This vulnerability also reportedly consumes excessive CPU resources.

- **Microsoft Internet Explorer COM Object Instantiation Buffer Overflow Vulnerability**

Microsoft Internet Explorer is prone to a buffer overflow vulnerability.

This issue is exposed when certain COM objects are instantiated as ActiveX controls. A malicious Web page could pass content to these objects that will trigger memory corruption.

Successful exploitation could let remote attackers execute arbitrary code in the context of the currently logged in user.

- **Microsoft Internet Explorer Web Folder Behaviors Cross-Domain Scripting Vulnerability**

Microsoft Internet Explorer is prone to a security vulnerability that may let a Web page execute malicious script code in the context of an arbitrary domain or browser security zone. This issue is the result of a security flaw in the browser security model when handling URIs when a Web folder view is rendered.

If exploited to access a foreign domain, this could allow script code embedded in a malicious Web page to access the properties of another site that the victim of the attack may trust. This would likely be exploited to steal credentials or sensitive information from the victim. The issue could also be exploited to execute arbitrary code by running malicious script code in a browser security zone with lowered security settings, such as the Local Machine, Trusted Sites or Intranet zone. Code execution would occur in the context of the currently logged in user.

- **Microsoft Windows Plug and Play Buffer Overflow Vulnerability**

Microsoft Windows Plug and Play is prone to a buffer overflow vulnerability.

This issue takes place when the PnP service handles malformed messages containing excessive data.

This vulnerability facilitates local privilege escalation and unauthorized remote access depending on the underlying operating system. A successful attack may result in arbitrary code execution resulting in an attacker gaining SYSTEM privileges.

UPDATE (8/23/2005): While performing further investigations into this vulnerability, the DeepSight Threat Analyst Team has been able to carry out anonymous remote exploitation against certain non-default configurations of Windows XP SP1. The attack vector manifests itself when the "Guest" account is both enabled and removed from the "Deny access to this computer from the network" entry in the "User Rights Assignment" Security Policy. This can happen when Simple File and Print Sharing has been enabled, for example by sharing a folder or a printer with the local network. It is important to note that Simple File and Print Sharing is only available on Windows XP machines that are not part of a Windows Active Directory Domain. However, configuring a Windows XP SP1 host to share network resources prior to joining an Active Directory Domain will leave it in the vulnerable state even after the Domain is joined.

It is also important to note that Windows XP SP2 is not susceptible to this exploitation method. Furthermore, there is no change to Microsoft Security Bulletin MS05-039. Customers who have deployed this update are protected from this issue.

In light of this finding, Microsoft has issued new information regarding the patch for the Microsoft Windows Plug and Play Buffer Overflow Vulnerability. More information is available in Microsoft Security Bulletin 906574 <http://www.microsoft.com/technet/security/advisory/906574.mspx>.

- **Microsoft Windows Print Spooler Buffer Overflow Vulnerability**

Microsoft Windows Print Spooler service is prone to a buffer overflow vulnerability.

Specifically, this issue takes place when the Print Spooler service handles malformed messages containing excessive data.

This vulnerability facilitates local privilege escalation and unauthorized remote access depending on the underlying operating system. A successful attack may result in arbitrary code execution, which can allow an attacker to gain SYSTEM privileges.

- **Microsoft Internet Explorer Unspecified SharePoint Portal Services Log Sink ActiveX Vulnerability**

Microsoft Internet Explorer is prone to an unspecified vulnerability in the SharePoint Portal Service Log Sink ActiveX control.

The vendor has not released any further information about this vulnerability other than to state the "kill bit" has been set on unsupported versions of the control.

- **Microsoft Windows Telephony Service Buffer Overflow Vulnerability**

Microsoft Windows Telephony Service is prone to a buffer overflow vulnerability. This issue is due to a failure in the application to perform proper bounds checking on user-supplied data.

A successful attack can result in overflowing a finite sized buffer and ultimately leading to arbitrary code execution in the context of the affected service. This may allow the attacker to execute arbitrary code remotely or locally to gain elevated privileges.

Remote code execution is only possible on Windows 2000 Server and Windows Server 2003; other vulnerable platforms the attacker must have local interactive access.

- **Microsoft Windows Kerberos Denial Of Service Vulnerability**

Microsoft Windows is susceptible to a remote Kerberos denial of service vulnerability. By sending unspecified packets to the Kerberos service on TCP or UDP port 88, attackers may cause the affected service to crash.

This vulnerability allows remote attackers to crash the affected authentication service, denying further domain authentication to legitimate users. It should be noted that exploitation requires that attackers have valid logon credentials.

- **Microsoft Windows Kerberos PKINIT Man In The Middle Vulnerability**

The PKINIT implementation in Microsoft Windows is susceptible to a man in the middle vulnerability. This issue is due to a failure of the software to properly validate network data. This issue is only exploitable by attackers that have access to valid logon credentials.

Attackers exploit this issue to spoof the domain controller/KDC during the initial authentication process. By spoofing the domain controller/KDC, attackers may gain access to the cleartext contents of encrypted network traffic in arbitrary Kerberos-enabled services. Other attacks may also be possible.

Microsoft implements draft 9 of the IETF PKINIT specification, and states that the vulnerability is in the protocol specification itself. Other implementations of PKINIT may therefore also be vulnerable to this issue.

- **Microsoft Hotfix Conflict Vulnerability**

The catalog file (Sp2.cat) within Windows 2000 Post-Service Pack 1 (English Version) Hotfixes has been improperly versioned. Previously implemented hotfixes can be uninstalled from a Windows 2000 machine, leaving the machine vulnerable to current security issues.

- **Microsoft IE Telnet Client File Overwrite Vulnerability**

Services for Unix 2.0 contains a client side logging option which records all information exchanged in a telnet session. A vulnerability exists that could enable a remote user to invoke the telnet client and execute arbitrary commands on a target machine via IE. This is achieved by crafting a URL composed of command line parameters to the telnet client, which would invoke 'telnet.exe'. Telnet would connect to the host and initate the logging of session information, access to this file will allow an attacker to write and execute arbitrary commands which may be executed later.

- **Microsoft IIS Various Domain User Account Access Vulnerability**

Microsoft IIS contains a flaw in the handling of FTP domain authentication.

A user attempting to authenticate using a valid login name appended with specially chosen characters, will not be required to specify the domain which the account belongs. The FTP service will instead search the domain and all trusted

domains for the user account. Once the account is located, the user will have to complete the authentication process. At this point brute force attacks can be used in an attempt to gain access to the domain.

- **Microsoft IIS MIME Header Denial of Service Vulnerability**

A flaw exists in version 5.0 of Microsoft IIS that makes it subject to a potential denial of service attack.

The problem occurs when the server is preparing the MIME headers for the response to a HTTP request for a certain type of file. Under certain circumstances, a failure causing the server to stop responding may occur.

In order for this vulnerability to be successfully exploited, a user would need appropriate permissions to add content to the web server.

No further technical details are available at this time.

- **Microsoft Windows XP Pro Upgrade IE Patch Downgrade Vulnerability**

A problem has been discovered in the Microsoft Windows XP Pro update procedure.

Users may expect that previously installed patches will carry over when they upgrade to Windows XP Pro from an earlier Microsoft operating system (such as Windows 98). However, it has been reported that previously installed patches for Internet Explorer 6.0 do not carry over when the upgrade is undertaken. Users may not be aware that they are running an unpatched version of Internet Explorer 6.0.

To complicate matters further, the previously installed patches are not available via the Windows Update service for XP Pro and must be sought out by the user.

This issue is known to affect upgrades to Windows XP Pro where the browser was a patched version of Internet Explorer 6.0. It is not known whether this affects other patched versions of Internet Explorer, or upgrades to other versions of the Microsoft operating system (such as Windows XP Home).

- **Microsoft Internet Explorer MIME Type File Extension Spoofing Vulnerability**
  Microsoft Internet Explorer uses the Content-Type and Content-Disposition HTML header fields to determine the file type of non-HTML files referenced by a website. These two content headers make up the MIME type of the field.
  It is possible to insert information into the Content-Type and Content-Disposition fields that would tell Internet Explorer that a file being downloaded is of a different type than it actually is. This would not cause the file to be executed automatically, but could trick a vulnerable user into believing that they are downloading a text file instead of an executable file.

This vulnerablility was originally believed to be the same as the one reported in Bugtraq ID 3597, but was later found to be a different method of achieving the same goal.

- **Microsoft Internet Explorer Known Local File Script Execution Vulnerability**

By default Microsoft Internet Explorer executes scripts from websites in the Internet Zone.

Due to a flaw in the way that Internet Explorer deals with cookies, it will execute any scripts embedded within a cookie in the Local Computer zone with the same privilege level as the currently logged in user.

It has been reported that this issue is based on the ability to force Internet Explorer to open arbitrary known files as HTML content. As a result, any local file which contains valid HTML or JavaScript may be rendered as such by the browser. Additional attack vectors beyond cookie files may exist.

Normally only files with the registered extensions .html or .htm will be interpreted as HTML content.

- **Microsoft IIS HTTP Redirect Cross Site Scripting Vulnerability**

A Cross Site Scripting issue exists in some versions of IIS. The HTTP Redirect page created by IIS may, under some circumstances, contain HTML content which includes unsanitized user supplied input.

A number of Cisco products are affected by this vulnerability, although this issue is not present in the Cisco products themselves.

- **Microsoft Internet Explorer Cookie Content Disclosure Vulnerability**

A flaw exists in the way that Microsoft Internet Explorer handles scripts embedded within cookies. Since cookies are essentially an extension of the website from which they were received, they should be treated as though they are in the Internet zone, and allowed access only to contents of their domain of origin.

However, some versions of Internet Explorer treat all cookie content as originating from the same domain. As a result, script code embedded in a cookie will have access to the contents of all cookies on the local machine.

New information suggests that Internet Explorer may still be vulnerable to this issue.

New reports suggest that it may be possible to embed encoded executable content within a cookie. If the cookie is then referenced as MHTML content through exploitation of this issue, it may prove possible to drop and execute arbitrary code on the vulnerable system. This possibility has not, however, been confirmed.

- **Microsoft IIS Administrative Pages Cross Site Scripting Vulnerabilities**

Microsoft IIS is prone to cross site scripting attacks. The vulnerability is a result of improper sanitization of user-supplied input by IIS. Several web pages, provided by IIS for administrative purposes do not adequately sanitize user-supplied input. Any malicious HTML code that may be included in the URI will be executed.

This vulnerability could allow an attacker to execute script code in the 'Intranet' security zone.

This vulnerability was originally described in BugTraq ID 6068. It is now being assigned its own BugTraq ID.

- **Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability**

It has been reported that Microsoft Windows Workstation (WKSSVC.DLL) service is prone to a vulnerability that may allow a remote attacker to gain unauthorized access to a vulnerable host. The problem is in the handling of requests by the Workstation Service. The Workstation Service does not properly check bounds on remote data therefore making it possible to overwrite sensitive regions of system memory.

- **Microsoft Jet Database Engine Remote Code Execution Vulnerability**

It has been reported that Microsoft Jet Database Engine (Jet) is prone to a remote code execution vulnerability that that may allow remote attackers to execute arbitrary code in order to gain unauthorized access to a vulnerable system. This issue presents itself when a specially crafted database query is sent by an attacker to be interpreted by Jet. A successful attack may allow the attacker to gain complete control of the affected system.

Microsoft Jet Database Engine version 4.0 running on various Microsoft operating systems is reported to be vulnerable to this issue.

- **Multiple Vendor TCP Sequence Number Approximation Vulnerability**

A vulnerability in TCP implementations has been reported that may permit unauthorized remote users to reset TCP sessions. This issue affects products released by multiple vendors. This issue may permit TCP sequence numbers to be more easily approximated by remote attackers.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range of the expected sequence number for a packet in the session. This will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those which have known or easily guessed IP address endpoints and those implementations with known or easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack. As a result, this issue is likely to affect a number of routing platforms.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

Other consequences may also result from this issue, such as injecting specific data in TCP sessions, though this has not been confirmed.

It is reported that Microsoft platforms are also prone to this vulnerability. Vendor reports indicate that an attacker will require knowledge of the IP address and port numbers of the source and destination of an existent legitimate TCP connection in order to exploit this vulnerability on Microsoft Platforms. Connections that involve persistent sessions, for example Border Gateway Protocol sessions, may be more exposed to this vulnerability than other TCP/IP sessions.

- **Microsoft Windows HSC DVD Driver Upgrade Code Execution Vulnerability**

A security vulnerability has been reported in Microsoft Windows XP and Server 2003 operating systems. This issue exists in the Help and Support Center (HSC) and is due to how the feature handles HCP invocation URIs for DVD driver upgrades.

This issue could be exploited from a malicious web page or HTML e-mail to cause a malicious executable to be run on a vulnerable system. This would occur in the context of the victim user, though it has been reported that significant user interaction is required for exploitation to occur.

While this issue may be exploited through Internet Explorer, it should also be noted that third-party web client software could also invoke HSC via a HCP URI.

- **Windows Kernel Font Buffer Overflow Vulnerability**

The Microsoft Windows Kernel is prone to a locally exploitable privilege escalation vulnerability. This issue is due to an unchecked buffer when handling malicious fonts, potentially allowing a local attacker to completely compromise a vulnerable computer.

Exploitation attempts could also result in a denial of service. Microsoft has reported that the vulnerability will most likely cause a denial of service on Windows XP SP2 platforms. The vendor has also stated that this vulnerability is

not critical on Windows 98/98SE/ME, possibly because of lack of multi-user support on the operating system.

- **Microsoft Windows Kernel Object Management Denial Of Service Vulnerability**
  The Microsoft Windows kernel is prone to a locally exploitable denial of service vulnerability. The issue is reportedly related to object management in the Windows kernel.

- **Microsoft Windows Message Queuing Remote Buffer Overflow Vulnerability**

A remote buffer overflow vulnerability affects Microsoft Windows. This issue is due to a failure of the affected functionality to properly validate the length of user-supplied strings prior to copying them into static process buffers. This vulnerability may be exploited over RPC.

An attacker may exploit this issue to execute arbitrary code with SYSTEM privileges, facilitating unauthorized access or privilege escalation.

It should be noted that MSMQ is not installed by default on affected platforms and must be manually installed for a computer to be vulnerable. The vulnerability is reportedly not present on computers that only enable MSMQ HTTP Message Delivery.

- **Microsoft Windows Kernel CSRSS Local Privilege Escalation Vulnerability**

A local privilege escalation vulnerability affects Microsoft Windows. This issue is due to a failure of the Kernel to properly handle user-supplied messages.

A local attacker may leverage this issue to completely compromise the computer.

- **Microsoft Windows Internet Protocol Validation Remote Code Execution Vulnerability**

Microsoft Windows is reported prone to a remote code execution vulnerability. It is reported that the vulnerability manifests when an affected Microsoft platform receives and processes an especially malformed TCP/IP packet.

Reports indicate that the immediate consequences of exploitation of this issue are a denial of service.

- **Microsoft Exchange Server SMTP Extended Verb Buffer Overflow Vulnerability**

Microsoft Exchange Server is prone to a buffer overflow in the X-LINK2STATE SMTP extended verb. Successful exploitation could result in arbitrary code execution.

- **Microsoft Windows Kernel Access Validation Request Buffer Overflow Vulnerability**

The Microsoft Windows kernel is prone to a buffer overflow in the system that validates access requests. Successful exploitation could allow arbitrary code execution in the context of the kernel. Only local users could exploit this vulnerability.

- **Multiple Vendor TCP/IP Implementation ICMP Remote Denial Of Service Vulnerabilities**

Multiple vendor implementations of TCP/IP Internet Control Message Protocol (ICMP) are reported prone to several denial of service attacks.

ICMP is employed by network nodes to determine certain automatic actions to take based on network failures reported by an ICMP message.

It is reported that for ICMP error messages, no security checks are recommended by the RFC. As long as an ICMP message contains a valid source and destination IP address and port pair, it will be accepted for an associated connection.

The following individual attacks are reported:

A blind connection-reset attack is reported to affect multiple vendors. This attack takes advantage of the specification that describes that on receiving a 'hard' ICMP error, the corresponding connection should be aborted. The Mitre ID CAN-2004-0790 is assigned to this issue.

A remote attacker may exploit this issue to terminate target TCP connections and deny service for legitimate users.

An ICMP Source Quench attack is reported to affect multiple vendors. This attack takes advantage of the specification that a host must react to receive ICMP Source Quench messages by slowing transmission on the associated connection. The Mitre ID CAN-2004-0791 is assigned to this issue.

A remote attacker may exploit this issue to degrade the performance of TCP connections and partially deny service for legitimate users.

An attack against ICMP PMTUD is reported to affect multiple vendors when they are configured to employ PMTUD. By sending a suitable forged ICMP message to a target host an attacker may reduce the MTU for a given connection. The Mitre ID CAN-2004-1060 is assigned to this issue.

A remote attacker may exploit this issue to degrade the performance of TCP connections and partially deny service for legitimate users.

It is reported that Microsoft platforms are also prone to these issues.

- **Microsoft Windows Shell Remote Code Execution Vulnerability**

Microsoft Windows is prone to a vulnerability that may allow remote attackers to execute code through the Windows Shell. The cause of the vulnerability is related to how the operating system handles unregistered file types. The specific issue is that files with an unknown extension may be opened with the application specified in the embedded CLSID.

The victim of the attack would be required to open a malicious file, possibly hosted on a Web site or sent through email. Social engineering would generally be required to entice the victim into opening the file.

- **Microsoft Windows Explorer Preview Pane Script Injection Vulnerability**

Microsoft Windows Explorer is prone to a script injection vulnerability. This occurs when the Windows Explorer preview pane (Web View) is enabled on Windows 2000 computers. Windows 98/98SE/ME are also affected by this issue. If a file with malicious attributes is selected using Explorer, script code contained in the attribute fields may be executed with the privilege level of the user that invoked Explorer. This could be exploited to gain unauthorized access to the vulnerable computer in the context of the currently logged in user.

- **Microsoft Windows HTML Help Remote Code Execution Vulnerability**

Microsoft Windows HTML Help is affected by a remote code execution vulnerability.

The vulnerability presents itself when the application handles malformed data through the InfoTech protocol (ms-its, its, mk:@msitstore).

An attacker may exploit this issue from a malicious Web page or through HTML email to execute arbitrary code with the privileges of the currently logged in user.

This vulnerability affects any application that utilizes the Windows Help component of Internet Explorer.

Security Update 25

Symantec NetRecon 3.6 Security Update 25 (SU25) detects and reports 15 new vulnerabilities.

New vulnerability detection

- **Microsoft IIS Administrative Pages Cross Site Scripting Vulnerabilities**
  Microsoft IIS is prone to cross site scripting attacks. The vulnerability is a result of improper sanitization of user-supplied input by IIS. Several web pages, provided by IIS for administrative purposes do not adequately

sanitize user-supplied input. Any malicious HTML code that may be included in the URI will be executed.

This vulnerability could allow an attacker to execute script code in the 'Intranet' security zone.

This vulnerability was originally described in BugTraq ID 6068. It is now being assigned its own BugTraq ID.

- **Microsoft IIS Various Domain User Account Access Vulnerability**
  Microsoft IIS contains a flaw in the handling of FTP domain authentication. A user attempting to authenticate using a valid login name appended with specially chosen characters, will not be required to specify the domain which the account belongs. The FTP service will instead search the domain and all trusted domains for the user account. Once the account is located, the user will have to complete the authentication process. At this point brute force attacks can be used in an attempt to gain access to the domain.

- **Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability**
  It has been reported that Microsoft Windows Workstation (WKSSVC.DLL) service is prone to a vulnerability that may allow a remote attacker to gain unauthorized access to a vulnerable host. The problem is in the handling of requests by the Workstation Service. The Workstation Service does not properly check bounds on remote data therefore making it possible to overwrite sensitive regions of system memory.

- **Microsoft Hotfix Conflict Vulnerability**
  The catalog file (Sp2.cat) within Windows 2000 Post-Service Pack 1 (English Version) Hotfixes has been improperly versioned. Previously implemented hotfixes can be uninstalled from a Windows 2000 machine, leaving the machine vulnerable to current security issues.

- **Microsoft IE Telnet Client File Overwrite Vulnerability**
  Services for Unix 2.0 contains a client side logging option which records all information exchanged in a telnet session. A vulnerability exists that could enable a remote user to invoke the telnet client and execute arbitrary commands on a target machine via IE. This is achieved by crafting a URL composed of command line parameters to the telnet client, which would invoke 'telnet.exe'. Telnet would connect to the host and initate the logging of session information, access to this file will allow an attacker to write and execute arbitrary commands which may be executed later.

- **Microsoft Windows XP Pro Upgrade IE Patch Downgrade Vulnerability**
  A problem has been discovered in the Microsoft Windows XP Pro update procedure.

  Users may expect that previously installed patches will carry over when they upgrade to Windows XP Pro from an earlier Microsoft operating

system (such as Windows 98). However, it has been reported that previously installed patches for Internet Explorer 6.0 do not carry over when the upgrade is undertaken. Users may not be aware that they are running an unpatched version of Internet Explorer 6.0.

To complicate matters further, the previously installed patches are not available via the Windows Update service for XP Pro and must be sought out by the user.

This issue is known to affect upgrades to Windows XP Pro where the browser was a patched version of Internet Explorer 6.0. It is not known whether this affects other patched versions of Internet Explorer, or upgrades to other versions of the Microsoft operating system (such as Windows XP Home).

- **Microsoft Internet Explorer Known Local File Script Execution Vulnerability**

  By default Microsoft Internet Explorer executes scripts from websites in the Internet Zone.

  Due to a flaw in the way that Internet Explorer deals with cookies, it will execute any scripts embedded within a cookie in the Local Computer zone with the same privilege level as the currently logged in user.

  It has been reported that this issue is based on the ability to force Internet Explorer to open arbitrary known files as HTML content. As a result, any local file which contains valid HTML or JavaScript may be rendered as such by the browser. Additional attack vectors beyond cookie files may exist.

  Normally only files with the registered extensions .html or .htm will be interpreted as HTML content.

- **Microsoft Internet Explorer Cookie Content Disclosure Vulnerability**

  A flaw exists in the way that Microsoft Internet Explorer handles scripts embedded within cookies. Since cookies are essentially an extension of the website from which they were received, they should be treated as though they are in the Internet zone, and allowed access only to contents of their domain of origin.

  However, some versions of Internet Explorer treat all cookie content as originating from the same domain. As a result, script code embedded in a cookie will have access to the contents of all cookies on the local machine.

  New information suggests that Internet Explorer may still be vulnerable to this issue.

  New reports suggest that it may be possible to embed encoded executable content within a cookie. If the cookie is then referenced as MHTML content through exploitation of this issue, it may prove possible to drop and execute arbitrary code on the vulnerable system. This possibility has not, however, been confirmed.

- **Microsoft Windows Logon Process Remote Buffer Overflow Vulnerability**
  Microsoft Windows logon process "winlogon" has been reported to be prone to a remote buffer overflow vulnerability. The issue is reported to exist when the vulnerable host is a member of an Active Directory domain. When processing logon information, the windows logon process will read data from the Active Directory. This read call does not sufficiently perform bounds checking on received data before said data is copied into a reserved buffer in process memory.
  Supplied data that exceeds the size of the allocated buffer in Windows logon process memory will overrun its bounds, this will result in the corruption of memory that is adjacent to the affected buffer.

- **Microsoft IIS HTTP Redirect Cross Site Scripting Vulnerability**
  A Cross Site Scripting issue exists in some versions of IIS. The HTTP Redirect page created by IIS may, under some circumstances, contain HTML content which includes unsanitized user supplied input.
  A number of Cisco products are affected by this vulnerability, although this issue is not present in the Cisco products themselves.

- **Microsoft Windows HSC DVD Driver Upgrade Code Execution Vulnerability**
  A security vulnerability has been reported in Microsoft Windows XP and Server 2003 operating systems. This issue exists in the Help and Support Center (HSC) and is due to how the feature handles HCP invocation URIs for DVD driver upgrades.
  This issue could be exploited from a malicious web page or HTML e-mail to cause a malicious executable to be run on a vulnerable system. This would occur in the context of the victim user, though it has been reported that significant user interaction is required for exploitation to occur.
  While this issue may be exploited through Internet Explorer, it should also be noted that third-party web client software could also invoke HSC via a HCP URI.

- **Microsoft Jet Database Engine Remote Code Execution Vulnerability**
  It has been reported that Microsoft Jet Database Engine (Jet) is prone to a remote code execution vulnerability that that may allow remote attackers to execute arbitrary code in order to gain unauthorized access to a vulnerable system. This issue presents itself when a specially crafted database query is sent by an attacker to be interpreted by Jet. A successful attack may allow the attacker to gain complete control of the affected system.
  Microsoft Jet Database Engine version 4.0 running on various Microsoft operating systems is reported to be vulnerable to this issue.

- **Microsoft IIS MIME Header Denial of Service Vulnerability**
  A flaw exists in version 5.0 of Microsoft IIS that makes it subject to a potential denial of service attack.
  The problem occurs when the server is preparing the MIME headers for the response to a HTTP request for a certain type of file. Under certain circumstances, a failure causing the server to stop responding may occur.
  In order for this vulnerability to be successfully exploited, a user would need appropriate permissions to add content to the web server.
  No further technical details are available at this time.

- **Microsoft Internet Explorer MIME Type File Extension Spoofing Vulnerability**
  Microsoft Internet Explorer uses the Content-Type and Content-Disposition HTML header fields to determine the file type of non-HTML files referenced by a website. These two content headers make up the MIME type of the field.
  It is possible to insert information into the Content-Type and Content-Disposition fields that would tell Internet Explorer that a file being downloaded is of a different type than it actually is. This would not cause the file to be executed automatically, but could trick a vulnerable user into believing that they are downloading a text file instead of an executable file.
  This vulnerablility was originally believed to be the same as the one reported in Bugtraq ID 3597, but was later found to be a different method of achieving the same goal.

- **Microsoft Windows ASN.1 Library Bit String Processing Variant Heap Corruption Vulnerability**
  Microsoft ASN.1 handling library has been reported prone to a heap corruption vulnerability. The issue presents itself in the ASN.1 bit string decoding routines, specifically the BERDecBitString() function. The issue manifests when the affected function attempts to process a constructed bit string that contain another nested constructed bit string.
  This vulnerability is exposed in a number of security related operating system components, including Kerberos (via UDP port 88), Microsoft IIS with SSL support enabled and NTLMv2 authentication (via TCP ports 135, 139 and 445). Other components may also be affected, though a comprehensive list is not available at this time. Client applications, which use the library, will be affected, including LSASS.EXE and CRYPT32.DLL (and any application that relies on CRYPT32.DLL). The vulnerable library is used frequently in components that handle certificates such as Internet Explorer and Outlook. Handling of signed ActiveX components could also present an exposure.

It should be noted that because ASN.1 data will likely be encoded, for example Kerberos, SSL, IPSec or Base64 encoded, the malicious integer values may be obfuscated and as a result not easily detectable.

Issues related to this vulnerability were originally covered in BID 9626 and 9743, further information has been made available which identifies that this is a distinct vulnerability in the library and so this specific issue has been assigned an individual BID.

June 5, 2005 Update: An IRC bot style tool may be exploiting this vulnerability. This alert will be updated as further information becomes available.

Security Update 24

Symantec NetRecon 3.6 Security Update 24 (SU24) detects and reports 3 new vulnerabilities.

New vulnerability detection

- **Cobalt Raq3 PopRelayD Arbitrary SMTP Relay Vulnerability**
  poprelayd is a script that parses /var/log/maillog for valid pop logins, and based upon the login of a client, allows the person logged into the pop3 service to also send email from the ip address they're accessing the system with.

  poprelayd doesn't authenticate output to the /var/log/maillog file. This makes it possible for a user to create an arbitrary string via sendmail that will be logged to the file, thus allowing a remote user to relay mail through the SMTP server.

- **Microsoft Windows 2000 SMTP Improper Authentication Vulnerability**
  Due to a flaw in the authentication process of the SMTP service in Windows 2000, it is possible for remote host to successfully authenticate and use the SMTP services as an authenticated user.

  This may lead to abuse of SMTP services, such as mass e-mail relaying.

- **NT Exchange Server Encapsulated SMTP Address Vulnerability**
  Microsoft Exchange Server 5.5 has a vulnerability that would allow an attacker to use any Internet-connected Exchange Server 5.5 (with at least one Internet Mail Service configured) as a mail relay by using encapsulated SMTP addresses. This vulnerability poses no threat to the data or software on the server, but could allow spam to be sent from the server without the administrator's knowledge or permission, and could lead to a Denial of Service condition if the volume of the mail relayed is sufficient.

Security Update 23

Symantec NetRecon 3.6 Security Update 23 (SU23) detects and reports 33 new vulnerabilities.

New vulnerability detection

- **Microsoft Internet Explorer Double Byte Character Set Handling Address Bar Spoofing Vulnerability**
  It is reported that Microsoft Internet Explorer is prone to a vulnerability that may allow a malicious Web page to spoof the address bar of the browser. This vulnerability presents itself due to a malfunction that occurs when certain double byte characters are encountered. As a result, this vulnerability will only affect computers that are configured to employ double byte character sets.
  This could be used to lure Web users into a false sense of trust since a malicious or spoofed site may pose as a site that is trusted by the user.
- **Microsoft Internet Explorer Function Pointer Override Cross-Domain Access Violation Vulnerability**
  Microsoft Internet Explorer is prone to an issue that could allow malicious script code to execute in a different domain.
  The Function Pointer Override method could be used to allow script code to execute on a vulnerable system in the security domain of a website in another browser window. This occurs due to a violation of the browser security zone policy.
  Further information has been made available stating that this issue was discovered by Liu Die Yu and publicly known prior to the release of MS03-048. This issue was originally described as one of the vulnerabilities in BID 8577 "Multiple Microsoft Internet Explorer Script Execution Vulnerabilities".
- **Microsoft Internet Explorer Bitmap Processing Integer Overflow Vulnerability**
  Microsoft Internet Explorer has been reported prone to an integer overflow vulnerability. The issue presents itself in bitmap file processing procedures and is due to the use of a signed integer employed during boundary checking routines.
  Ultimately an attacker may exploit this condition to corrupt a saved instruction or stack frame base pointer, to influence execution flow of the affected browser into attacker-supplied instructions.
  This issue could also be exposed via other software that uses Internet Explorer to render images, such as Outlook, though this has not been confirmed.

- **Microsoft Internet Explorer Double-Null URI Denial Of Service Vulnerability**
  A problem in the handling of URIs with double nulls has been reported in Microsoft Internet Explorer. Because of this, it may be possible for a remote attacker to deny service to legitimate users of an affected system.
  Additionally, this option is conjectured to be an issue in a library component within the browser, as this issue affects Microsoft Internet Explorer and Microsoft Outlook. This would also likely affect any other system components that invoke the browser.

- **Microsoft Internet Explorer ExecCommand Cross-Domain Access Violation Vulnerability**
  Microsoft Internet Explorer is prone to an issue that could allow malicious script code to execute in a different domain.
  The ExecCommand method could be used to allow script code to execute on a vulnerable system in the security domain of a website in another browser window. This occurs due to a violation of the browser security zone policy.
  Further information has been made available stating that this issue was discovered by Liu Die Yu and publicly known prior to the release of MS03-048. This issue was originally described as one of the vulnerabilities in BID 8577 "Multiple Microsoft Internet Explorer Script Execution Vulnerabilities".

- **Microsoft Internet Explorer Heartbeat ActiveX Control Unspecified Vulnerability**
  An unspecified vulnerability exists in the Microsoft Internet Explorer Heartbeat MSN gaming ActiveX control (heartbeat.ocx).

- **Microsoft Internet Explorer Implicit Drag and Drop File Installation Vulnerability**
  Microsoft Internet Explorer is reported prone to a vulnerability that may allow unauthorized installation of malicious executables. Proof-of-concepts have been released to demonstrate a vulnerability that may be exploited to entice a victim user to install a file on a victim's computer with some degree of user interaction.
  Specifically, an executable may be embedded in a Web page and presented as an image object to the user. Another frame can be loaded that references a folder on the victim's file system via the anchorClick style behavior. The page will be obfuscated in such a way as to disguise the fact that when the user clicks on the image object it will implicitly drag it to the folder that has been specified.
  It has been demonstrated that various other measures may be taken to limit the amount of user interaction required but the exploit hinges on the user interacting via mouse events with an object within the Web page that

represents an executable to cause the executable to be moved to the folder that has been loaded in the obfuscated secondary frame.

An attacker may exploit this vulnerability to influence a target victim into unknowingly installing software in a location on the computer such as the startup foler. If the malicious executable is placed in the startup folder, it will run when the system is restarted.

- **Microsoft Internet Explorer Install Engine ActiveX Control Buffer Overflow Vulnerability**

  A remotely exploitable buffer overflow vulnerability exists in the Microsoft Internet Explorer Install Engine ActiveX control. This vulnerability is caused by insufficient bounds checking of arguments passed to the control.

  The vulnerability may be exploited to execute arbitrary code in the context of the client user.

  ** Update: NGSSoftware has released a preliminary advisory for this issue announcing that technical details will be withheld until January 19th, 2005.

- **Microsoft Internet Explorer Malformed GIF Double Free Code Execution Vulnerability**

  Microsoft Internet Explorer is reported prone to a double free memory corruption vulnerability when processing a malformed GIF image file. This vulnerability may potentially be exploited to execute arbitrary code in the context of the currently logged in user. Exploitation attempts could also cause a denial of service.

  To exploit this issue, an attacker could create a malicious GIF file and entice a user to view the file through Internet Explorer. Other applications that support the GIF format may also be affected, though this has not been confirmed.

  An attacker could exploit this issue through various means, such as enticing a user to visit a Web page that references the malicious file or through HTML email.

- **Microsoft Internet Explorer Method Caching Mouse Click Event Hijacking Vulnerability**

  In BID 8577 and 9009, it was reported that by using a DHTML method an attacker could potentially hijack mouse click events and influence an Internet Explorer user into invoking unintended procedures. This earlier vulnerability was previously addressed by MS03-048.

  It has been reported that a variation on the previous vulnerability has been discovered that will bypass security measures implemented in MS03-048. By using DHTML method caching functions an attacker may make the moveBy() method of the window object available and so may potentially hijack mouse click events to simulate a drag and drop operation. This attack may also apply to the moveTo(), resizeBy(), and resizeTo() methods of the window object.

Like the earlier vulnerability, this could be exploited to place an executable on the victim's system in such a way that it may be run at a later time. This would result in execution of arbitrary code in the context of the victim user.

- **Microsoft Internet Explorer Modal Dialog Zone Bypass Vulnerability**
  Microsoft Internet Explorer is prone to a vulnerability that may permit cross-zone access, allowing an attacker to execute malicious script code in the context of the Local Zone. It is possible to exploit this issue by passing a dynamically created IFrame to a modal dialog.
  This vulnerability could be exploited in combination with a number of other security issues, such as the weakness described in BID 10472. The end result of successful exploitation is execution of arbitrary code in the context of the client user.
  It may also be possible to exploit this vulnerability to access properties of a foreign domain, allowing for other types of attacks that compromise sensitive or private information associated with a domain of the attacker's choosing.

- **Microsoft Internet Explorer Mouse Click Event Hijacking Vulnerability**
  A vulnerability exists in Internet Explorer when handling specific DHTML events, allowing a malicious Web page to intercept mouse click events to perform unintended drag and drop operations.
  In particular, it is possible to simulate a mouse drag and drop event through use of the moveBy() DHTML method of the window object. This attack may also apply to the moveTo(), resizeBy(), and resizeTo() methods of the window object. This could be exploited by creating a link that when clicked will cause an object such as an executable or shortcut to be stored on the client computer, such as in the startup folder.
  Successful exploitation will permit execution of arbitrary code in the context of the client user.
  It should be noted that a later variant of this issue exists (BID 9108) that evades the fixes provided in MS03-048. This later variant is addressed by MS04-004.

- **Microsoft Internet Explorer NavigateAndFind() Cross-Zone Policy Vulnerability**
  A vulnerability has been reported in Microsoft Internet Explorer. Because of this, an attacker may be able to violate cross-zone policy.
  It has been reported that the issue presents itself due to a failure by Internet Explorer to remove JavaScript URIs from the browser history list in some circumstances. A JavaScript specific JavaScript URI, can be embedded in the Browser history list and further employed by an attacker to have JavaScript code executed in the context of the Local Machine security zone.
  This issue is similar in nature to the vulnerability described in BID 9109.

- **Microsoft Internet Explorer OBJECT Tag Buffer Overflow Vulnerability**
  Microsoft Internet Explorer is prone to a boundary condition error when handling OBJECT tags in web pages. When a web page containing an OBJECT tag using a parameter containing excessive data is encountered by a vulnerable client, a internal memory buffer will be overrun. This could cause Internet Explorer to fail or potentially result in the execution arbitrary code in the security context of the current user.
- **Microsoft Internet Explorer Plug-in Navigations Handling Address Bar Spoofing Vulnerability**
  It is reported that Microsoft Internet Explorer is prone to a vulnerability that may allow a malicious Web page containing embedded flash multimedia to spoof the address bar of the browser.
  This could be used to lure Web users into a false sense of trust since a malicious or spoofed site may pose as a site that is trusted by the user.
- **Microsoft Internet Explorer Popup.show Mouse Event Hijacking Vulnerability**
  A vulnerability exists in Microsoft Internet Explorer that may permit a malicious Web page to hijack mouse events. This could potentially be exploited to trick an unsuspecting user into performing unintended actions such as approving pop-up dialogs.
  The method caching variant of this attack is also reported to work.
  This is similar to the vulnerability described in BID 9108.
  This issue could potentially be exploited to execute arbitrary code or be used in other attacks.
- **Microsoft Internet Explorer Script URL Cross-Domain Access Violation Vulnerability**
  Microsoft Internet Explorer is prone to an issue that could allow malicious script code from one domain to execute in the context of different domain.
  The Script URL method could be used to allow script code to execute on a vulnerable system in the security domain of a website in another browser window. This occurs due to a violation of the browser security zone policy. According to Microsoft, this vulnerability can be exploited by attackers to run arbitrary exectuables on victim hosts. This would also permit malicious scripts to gain access to properties of documents in foreign domains.
  This BID encapsulates a number of previously known issues discovered by Liu Die Yu and Jelmer. These issues are also described in BIDs 8577, 9769 and 9798.
- **Microsoft Internet Explorer Secure Sockets Layer Caching Vulnerability**
  Microsoft Internet Explorer is reported prone to a Secure Sockets Layer caching vulnerability.

It is reported that arbitrary content may be cached to the computer that is viewing a malicious site when this vulnerability is exploited. This cached content will be rendered in the context of a legitimate site when a legitimate site is viewed.

- **Microsoft Internet Explorer Style Tag Comment Memory Corruption Vulnerability**
  A heap overflow vulnerability has been discovered in Internet Explorer. It is reported that the issue presents itself when a comment character sequence that is not terminated is encountered after a STYLE tag.
  This issue could be exploited by a remote attacker to execute arbitrary code in the context of the client user. The attacker would likely create a malicious HTML page and host it on a site. The attacker would then attempt to entice a user to visit the malicious page to carry out a successful attack.

- **Microsoft Internet Explorer Unspecified showHelp Zone Bypass Vulnerability**
  Microsoft Security Bulletin MS04-038 includes fixes to address an unspecified vulnerability in Internet Explorer that may permit elevation of zone privileges by bypassing from the Internet Zone to the Local Zone.
  The vendor has stated that additional security verifications have been added to prevent the showHelp DHTML method from being abused by a malicious Web site to load HTML Help files in the context of the Local Zone. It is unclear at this point whether they mean HTML Help files that already exist on the system or HTML Help files that originate from a remote source.
  Although unconfirmed, this could be related to the following unspecified vulnerability that was addressed in Windows XP SP2/BID 10897 (Microsoft Windows XP SP2 Released - Multiple Vulnerabilities Fixed):
  - HTML Help Update to Limit Functionality When It Is Invoked with the window.showHelp( ) Method
  This is likely similar to earlier issues that have been reported in showHelp, such as BID 9320. Microsoft has not released further details about this vulnerability.

- **Microsoft Internet Explorer window.open Media Bar Cross-Zone Scripting Vulnerability**
  It has been reported that Microsoft Internet Explorer may be prone to a cross-zone scripting vulnerability that could ultimately lead to execution of malicious script code and Active Content in the context of the My Computer Zone or a foreign domain. Reportedly, hostile code can be executed in the context of the Media Bar via the '_media' property of the 'window.open' method. Cross-Site scripting attacks are possible as well. This functionality is only available in Internet Explorer 6 and above.
  This issue was originally described in BID 8577 "Multiple Microsoft Internet Explorer Script Execution Vulnerabilities".

- **Microsoft Internet Explorer XML Object Zone Restriction Bypass Vulnerability**
  Microsoft has announced that a vulnerability exists in Internet Explorer when handling malicious XML objects. The problem is said to occur due to Internet Explorer failing to validate a supplied path when binding local data to the XML document. As a result, a malicious HTML containing an embedded XML objects may be capable of exposing the contents of the local filesystem, despite the object being within the Internet or Intranet zone.

- **Microsoft Outlook Express Malformed Email Header Denial Of Service Vulnerability**
  Microsoft Outlook Express is prone to a security vulnerability when processing emails with malformed header data. A remote attacker may potentially exploit this issue to cause a persistent denial of service in the email client.
  This issue is only reported to affect Outlook Express 6.0 on Windows XP platforms.

- **Microsoft Window Management API Local Privilege Escalation Vulnerability**
  Microsoft has reported that several unspecified Window Management API functions can allow a local attacker to change the attributes of an application with higher level of privileges. This can allow the attacker to gain elevated privileges on a vulnerable computer.
  This issue represents a fundamental design flaw, as certain messages used to communicate between windows on a desktop may adversely affect the operation of a receiving process. By altering various properties of window components running with higher privileges, an attacker can create circumstances where attacks such as buffer overflows and potential arbitrary code execution are possible.
  This issue likely affects some native Windows applications but other third-party applications may also provide an opportunity for exploitation.

- **Microsoft Windows Kernel Local Denial of Service Vulnerability**
  The Microsoft Windows kernel is prone to a denial of service vulnerability. This issue can allow a local attacker to cause a vulnerable computer to stop responding and restart. This can effectively deny service to legitimate users.
  This issue does not pose a privilege escalation threat.

- **Microsoft Windows Kernel Virtual DOS Machine Privilege Escalation Vulnerability**
  Microsoft Windows Kernel Virtual DOS Machine is reported prone to a local privilege escalation vulnerability.
  The Microsoft Virtual DOS Machine (VDM) is a protected environment that emulates MS-DOS on Windows NT-based operating systems. This issue

arises due to an access validation error. A local attacker can exploit this vulnerability to gain elevated privileges on a vulnerable computer.

- **Microsoft Windows Media Player Automatic File Download and Execution Vulnerability**
  It has been reported that Windows Media Player allows for the automatic downloading and execution of files. This is done using a specifically crafted XMLNS (XML Name Space) URI embedded within an HTML email message. This is combined with the vulnerability described in BID 5543 to allow Windows Media Player to download and execute the referenced file without user intervention.

- **Microsoft Windows Media Player IE Zone Access Control Bypass Vulnerability**
  It has been reported by a reliable source that a method exists for evading the Zone based access control model used by Microsoft Internet Explorer. This technique reportedly relies on a flaw in Windows Media Player that allows for untrusted content to access the Local Zone.

- **Microsoft Windows NetDDE Remote Buffer Overflow Vulnerability**
  Microsoft Windows NetDDE is affected by a remote buffer overflow vulnerability. This issue is due to a failure of the application to properly verify the lengths of strings contained within unspecified network messages prior to copying them into finite buffers.
  It should be noted that NetDDE is not activated by default on Windows computers.
  An attacker may leverage this issue to execute arbitrary code on an affected computer with SYSTEM privileges. It is also noted that in some circumstances, where NetDDE services have been installed but not started, local attackers might exploit this issue to gain elevated privileges since it may be possible for an unprivileged user to start the services.
  ** Update: NGSSoftware has released a preliminary advisory for this issue announcing that technical details will be withheld until January 19th, 2005.
  ** Update: Immunity Research has reported that a remote attacker may require authentication prior to the exploitation of this vulnerability. Further details of this report can be found in the referenced message "ms04-031 pre-auth ??".

- **Microsoft Windows Program Group Converter Filename Local Buffer Overrun Vulnerability**
  Microsoft Windows Program Group Converter (grpconv.exe) is reported prone to a buffer overrun vulnerability. The issue is reported to exist due to a lack of sufficient validation performed on filename data.
  An attacker may craft a malicious file and present it to a victim in order to exploit this vulnerability. Additionally, it is demonstrated that this

vulnerability may also be exploited using a series of seperate vulnerabilities in Internet Explorer in order to exploit this vulnerability when a malicious website is viewed.

It is reported that exploitation may be hindered because parameter data is stored in Unicode format.

- **Microsoft Windows Shell Long Share Name Buffer Overrun Vulnerability**
  Microsoft Windows operating systems have been reported to be prone to a remotely exploitable buffer overrun condition.

  This issue is exposed when a client attempts to connect to an SMB share with an overly long name. This may cause explorer.exe or Internet Explorer to crash but could also potentially be leveraged to execute arbitrary code as the client user.

- **Microsoft Windows WMF/EMF Image Format Rendering Remote Buffer Overflow Vulnerability**
  Microsoft Windows WMF/EMF image rendering library is affected by a remote buffer overflow vulnerability. This issue is due to a failure of the affected library to properly verify the lengths of strings contained within an affected image file prior to copying them into finite buffers.

  Any code execution that occurs will take place with SYSTEM privileges due to the nature of the affected library. This will also permit local privilege escalation attacks.

- **Multiple Microsoft Internet Explorer Script Execution Vulnerabilities**
  Multiple issues have been reported in Microsoft Internet Explorer. Though these issues have been reported by a reliable source, communication issues have presented difficulty in obtaining details surrounding the reported issues. This vulnerability entry will be updated when additional information becomes available.

  *** Further information has been made available stating that MS03-048 includes updates to address some of these issues. The particular issues are also covered in BIDs 9013, 9014 and 9015.

  Specific details about two of these issues are included in BIDs 9769 and 9798.

  *** BID 10514 has been created to reflect specific information regarding the ADODB.Stream Object exploit.

Security Update 22

Symantec NetRecon 3.6 Security Update 22 (SU 22) detects and reports 8 new vulnerabilities.

New vulnerability detection

- **Apache ap_escape_html Memory Allocation Denial Of Service Vulnerability**
  Apache Web Server is reportedly affected by a memory allocation based denial of service vulnerability. This issue is due to a failure of the server to handle excessivley long HTTP header strings.
  This issue would allow an attacker to cause the affected application to crash, denying service to legitimate users.
  Although Apache version 2.0.49 reportedly affected by this issue, it is likely that earlier versions are affected as well.

- **Apache mod_ssl Denial Of Service Vulnerability**
  Apache mod_ssl is reported susceptible to a denial of service vulnerability.
  This issue presents itself during SSL connections to a vulnerable Apache server. The affected software may enter into an infinite loop in certain circumstances. This will consume CPU resources and potentially cause further connections to the affected server to fail.
  All Apache versions from 2.0 through to 2.0.50 are reported vulnerable.
  Update: Avaya has released an advisory identifying Avaya S8700/S8500/S8300 running CM 2.0 and later, and all versions of Avaya Converged Communication Server as vulnerable to this issue.

- **Apache Mod_SSL Log Function Format String Vulnerability**
  Reportedly mod_ssl is affected by a format string vulnerability within its logging function. This issue is due to a failure of the application to properly implement a formatted string function.
  Successful exploitation of this issue will most likely allow an attacker to gain control of the execution flow of the affected process and execute arbitrary code on the affect computer. It should be noted that although this quite likely, it has not been verified.

- **Apache Web Server Configuration File Environment Variable Local Buffer Overflow**
  Reportedly the Apache Web Server is affected by a configuration file environment variable local buffer overflow vulnerability. This issue is due to a failure of the affected application to validate user-supplied string lengths before copying them into finite process buffers.
  An attacker may leverage this issue to execute arbitrary code on the affected computer with the privileges of the Apache Web Server process.

- **Apache Web Server Remote IPv6 Buffer Overflow Vulnerability**
  Apache Web Server is reportedly affected by a remote buffer overflow vulnerability. This issue is due to a buffer boundary condition error that fails to provide a valid string length parameter while using libc memory copy functions.

It has been reported that this issue can be exploited to execute arbitrary code on computers running BSD based Unix variants. This issue is reportedly due to the implementation of the 'memcpy()' function.

On Linux based Unix variants this issue can only be exploited to trigger a denial of service condition.

- **Microsoft Internet Explorer JavaScript Method Assignment Cross-Domain Scripting**

  A vulnerability exists in Microsoft Internet Explorer that may allow cross-domain scripting.

  It is reported that the vulnerability presents itself due to a failure to properly validate trust relationships between method calls that are made in separate Internet Explorer windows. This may make it possible for script code to access properties of a foreign domain.

  This issue may also potentially be exploited to cross Security Zone boundaries, though this has not been confirmed.

- **MySQL Mysql_real_connect Function Potential Remote Buffer Overflow**

  MySQL is prone to a potential remote buffer overflow vulnerability. This issue occurs due to insufficient boundary checks performed by the 'mysql_real_connect' function.

  The 'mysql_real_connect' function does not verify the length of the IP address returned through a DNS response from a server. Immediate consequences of an attack may result in a denial of service condition. It is conjectured that this issue could allow for arbitrary code execution, however, this has not been confirmed.

  It is also reported that the glibc library verifies the length of an IP address, however, other libraries may obtain the length from a DNS response packet. Computers using glibc on Linux and BSD platforms may not be vulnerable to this issue.

- **PHP Strip_Tags() Function Bypass Vulnerability**

  It is reported that it is possible to bypass PHPs strip_tags() function.

  It is reported that under certain circumstances, PHPs strip_tags() function will improperly leave malformed tags in place.

  This vulnerability may mean that previously presumed-safe web applications could contain multiple cross-site scripting and HTML injection vulnerabilities when viewed by Microsoft Internet Explorer or Apple Safari web browsers.

  It is reported that 'magic_quotes_gpc' must be off for PHP to be vulnerable to this issue.

Security Update 21

Symantec NetRecon 3.6 Security Update 21 (SU 21) detects and reports 8 new vulnerabilities.

New vulnerability detection

- **ISC Bind 4 nslookupComplain() Buffer Overflow Vulnerability**
  BIND is a server program that implements the domain name service protocol. It is in extremely wide use on the Internet, in use by most of the DNS servers. Version 4 of BIND contains a stack overflow that may be exploitable to remote attackers. The vulnerability is due to unsafe use of the sprintf() function to construct an error message.
  If an attacker controls a DNS server, this vulnerability can be exploited. An attacker may be able to execute shellcode with the privileges of named (typically root).
- **ISC Bind 4 nslookupComplain() Format String Vulnerability**
  BIND is a server program that implements the domain name service protocol. It is in extremely wide use on the Internet, in use by most of the DNS servers. Version 4 of BIND contains a format string vulnerability that may be exploitable to remote attackers.
  The format string is in the nsloookupComplain() function, which creates an error message and logs it via syslog().
  If an attacker controls a DNS server, this vulnerability may be exploitable. An attacker may be able to execute shellcode with the privileges of named (typically root).
- **ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability**
  BIND is a server program that implements the domain name service protocol. It is in extremely wide use on the Internet, in use by most of the DNS servers. Version 8 of BIND contains a overflow that may be exploitable to remote attackers. Due to a bug that is present when handling invalid transaction signatures, it is possible to overwrite some memory locations with a known value. If the request came in via the UDP transport then the area partially overwriten is a stack frame in named. If the request came in via the TCP transport then the area partically overwriten is in the heap and overwrites malloc's internal variables. This can be exploited to execute shellcode with the privileges of named (typically root).
- **ISC BIND Internal Memory Disclosure Vulnerability**
  BIND is a server program that implements the domain name service protocol. It is in extremely wide use on the Internet, in use by most of the DNS servers.

It is believed that most (if not all) versions of BIND in use contain a vulnerability that may allow an attacker to view named's memory.

This may aid an attacker in further attacks.

- **OpenSSL Denial of Service Vulnerabilities**
  Three security vulnerabilities have been reported to affect OpenSSL. Each of these remotely exploitable issues may result in a denial of service in applications which use OpenSSL.

  The first vulnerability is a NULL pointer assignment that can be triggered by attackers during SSL/TLS handshake exchanges. The CVE candidate name for this vulnerability is CAN-2004-0079. Versions 0.9.6c to 0.9.6k (inclusive) and from 0.9.7a to 0.9.7c (inclusive) are vulnerable.

  The second vulnerability is also exploited during the SSL/TLS handshake, though only when Kerberos ciphersuites are in use. The vendor has reported that this vulnerability may not be a threat to many as it is only present when Kerberos ciphersuites are in use, an uncommon configuration. The CVE candidate name for this vulnerability is CAN-2004-0112. Versions 0.9.7a, 0.9.7b, and 0.9.7c are affected.

  This entry will be retired when individual BID records are created for each issue.

  Note: A third denial of service vulnerability included in the announcement was discovered affecting 0.9.6 and fixed in 0.9.6d. The CVE candidate name for this vulnerability is CAN-2004-0081.

- **PHP memory_limit Remote Code Execution Vulnerability**
  Reportedly PHP modules compiled with memory_limit support are affected by a remote code execution vulnerability. This issue is due to a failure of the PHP module to properly handle memory_limit request termination.

  This issue is reportedly exploitable by exploiting the Apache ap_escape_html Memory Allocation Denial Of Service Vulnerability (BID 10619); an attacker can cause premature termination during critical code execution. It should be noted that although the above-mentioned Apache vulnerability is the only known attack vector, there might be other attack vectors that are currently unknown.

  An attacker can exploit this issue to execute arbitrary code on an affected computer within the context of the vulnerable application, facilitating unauthorized access.

- **Samba Filename Mangling Method Buffer Overrun Vulnerability**
  Samba is reported prone to an undisclosed buffer overrun vulnerability, the buffer overrun is reported to exist when Samba is handling file name mangling with the "hash" method.

  It is conjectured that this vulnerability may present itself when the affected server handles a filename that is sufficient to trigger the vulnerability. To

exploit this vulnerability, an attacker may require sufficient access so that they may write a file to a published samba share.

It is reported that the vulnerability does not exist in default Samba configurations; by default, Samba is configured to employ "hash2" name mangling. The "hash2" method is not vulnerable.

This vulnerability is reported to affect Samba version 3.0.0 and later.

- **Samba Web Administration Tool Base64 Decoder Buffer Overflow Vulnerability**

  It has been reported that Samba Web Administration Tool (SWAT) is affected by a base64 decoder buffer overflow vulnerability. This issue is due to a failure of the application to properly validate buffer boundaries when copying user-supplied input into a finite buffer.

  Successful exploitation of this issue will allow a remote, unauthenticated attacker to execute arbitrary code on the affected computer with the privileges of the affected process; Samba typically runs with superuser privileges.

Security Update 20

Symantec NetRecon 3.6 Security Update 20 (SU 20) detects and reports 8 new vulnerabilities.

New vulnerability detection

- **HP Web Jetadmin Printer Firmware Update Script Arbitrary File Upload Weakness**
  HP Web Jetadmin is prone to an issue which may permit remote users to upload arbitrary files to the management server.
  This issue exists in the printer firmware update script. Given the ability to place arbitrary files on the server to an attacker-specified location, it may be possible to execute arbitrary code, though this will require exploitation of other known vulnerabilities, such as BID 9972 "HP Web Jetadmin setinfo.hts Script Directory Traversal Vulnerability".
  Authentication, if it has been enabled, would be required to exploit this issue.
  This issue was reported in HP Web Jetadmin version 7.5.2546 on a Windows platform. Other versions may be similarly affected.
- **HP Web Jetadmin setinfo.hts Script Directory Traversal Vulnerability**
  It has been reported that HP Web JetAdmin may be prone to a directory traversal vulnerability allowing remote attackers to access information outside the server root directory. The problem exists due to insufficient sanitization of user-supplied data passed via the 'setinclude' parameter of 'setinfo.hts' script.
  This vulnerability can be combined with HP Web Jetadmin Firmware Update Script Arbitrary File Upload Weakness (BID 9971) to upload malicious files to a vulnerable server in order to gain unauthorized access to a host.
  This issue has been tested with an authenticated account on HP Web Jetadmin version 7.5.2546 running on a Windows platform.
- **HP Web Jetadmin Remote Arbitrary Command Execution Vulnerability**
  Reportedly HP web Jetadmin is prone to a remote arbitrary command execution vulnerability. This issue is due to a failure of the application to properly validate and sanitize user supplied input.
  Successful exploitation of this issue will allow a malicious user to execute arbitrary commands on the affected system.
  This issue has been tested with an authenticated account on HP Web Jetadmin version 7.5.2546 running on a Windows platform.

- **HP Web Jetadmin Multiple Vulnerabilities**
  Multiple vulnerabilities have been identified in the application that may allow remote attackers to disclose sensitive information, carry out denial of service attacks, and gain unauthorized access to a vulnerable server.
  These issues are reported to affect HP Web JetAdmin 6.5 and prior, however, version 7.0 may be affected by most of these issues as well.

- **Microsoft Internet Explorer Shell: IFrame Cross-Zone Scripting Vulnerability**
  It has been alleged that Microsoft Internet Explorer is prone to a weakness that may potentially allow for the execution of hostile script code in the context of the My Computer Zone. This issue is related to how shell: URIs are handled by the browser. It should also be noted that shell: URIs may be used to reference local content in the same manner as file:// URIs.
  Update: Although unconfirmed, further reports indicate that MSN messenger version 6.2.0137, Microsoft Word, Outlook 2003, and Outlook Express may also potentially provide exploitation vectors for this vulnerability.

- **Microsoft Windows Shell CLSID File Extension Misrepresentation Vulnerability**
  A vulnerability has been reported in the Windows Shell that may allow files to be misrepresented to client users. The reported vulnerability involves specifying the CLSID for HTML applications in the name of a malicious file, followed by another file name and extension.
  This issue could be exploited to disguise executable content in the form of an HTML application (HTA) file as a file type that may appear innocuous to a victim user, such as a media file. The file will appear to be of an attacker-specified type in the file download dialog presented to the user. The user may then download/open that file under the assumption it is safe, which could result in execution of malicious code on the client system in the context of the victim user. A proof-of-concept was released which creates an embedded web interface to play a media file, which could further convince the user to open the malicious HTML application.

- **Microsoft Windows HTML Help Heap Overflow Vulnerability**
  The Microsoft Windows HTML Help facility is prone to a remotely exploitable heap overflow vulnerability. This vulnerability could be exploited from a malicious Web page or through HTML email to execute arbitrary code with the privileges of the currently logged in user.

- **Microsoft Windows Task Scheduler Remote Buffer Overflow Vulnerability**
  Microsoft Task Scheduler is reported prone to a remote stack-based buffer overflow vulnerability. The source of the vulnerability is that data in '.job' files is copied into an internal buffer without sufficient bounds checking.

It is reported that a remote attacker may exploit this vulnerability through Internet Explorer or Windows Explorer when the '.job' file is opened or a directory containing the file is rendered. The file could also be hosted on a share. Other attack vectors may also exist.

It should be noted that while this issue does not affect Windows NT 4.0 SP6a, it may affect this platform if Internet Explorer 6 SP1 is installed.

Security Update 19

Symantec NetRecon 3.6 Security Update 19 (SU 19) detects and reports 17 new vulnerabilities.

New vulnerability detection

- **Cisco Catalyst 2900 VLAN Vulnerability**

  This is an apparent design flaw in the 802.1q specification when deployed in VLAN's with Cisco Catalyst switches. The discussion which follows is taken from the original message which is credited and contained in its entirety later within this vulnerability entry. Virtual LAN (VLAN) technology is used to create logically separate LANs on the same physical switch. Each port of the switch is assigned to a VLAN. In the case of the Cisco Catalyst, VLAN'ing is done at layer 2 of the OSI network model, which means that a layer 3 device (router) is required to get traffic between VLANs (possibly a filtering device).

  VLANs may be extended beyond a single switch through the use of trunking between the switches. The trunk allows VLANs to exist on multiple switches. To preserve VLAN information across the trunk, the ethernet frame is 'wrapped' in a trunking protocol. Cisco have their own proprietary trunking protocol, but they also support the emerging 802.1q standard - we used 802.1q trunking in these tests. Basically, 802.1q adds a tag to the ethernet frame that specifies the VLAN that the frame belongs to. Thus, when it is transported between switches over the trunk, it is possible for the receiving switch to send the frame to the correct VLAN. In Cisco's implementation of 802.1q the tag is four bytes long and has the format "0x 80 00 0n nn" where nnn is the VLAN identifier. The tag is inserted into the ethernet frame immediately after the source MAC address. So, an ethernet frame entering switch 1 on a port that belongs to VLAN 4 has the tag "80 00 00 04" inserted. The 802.1q frame traverses the switch trunk and the tag is stripped from the frame before the frame leaves the destination switch port.

  For more information on 802.1q - http://grouper.ieee.org/groups/802/1/vlan.html

During our tests we used the packet generation tool of Network Associates' Sniffer Pro v 2 to generate 802.1q frames with modified VLAN identifiers in an attempt to get frames to hops VLANs without the intervention of a layer 3 device. We found that under specific conditions it was possible to inject frames into one VLAN and have them 'hop' to a different VLAN. This is a serious concern if the VLAN mechanism is being used to maintain a security gradient between two network segments. This has been discussed with Cisco and we believe that it is an issue with the 802.1q specification rather than an implementation issue. The trunk port, along with all the other ports, must be assigned to a VLAN. If some non-trunk ports on the switch share the same VLAN as the trunk port, then it is possible to inject modified 802.1q frames into these non-trunk ports, and have the frames hop to other VLANs on another switch. For example, Switch 1 has ports 1-12 on VLAN 1 Switch 1 has ports 13-23 on VLAN 2 Switch 1 has port 24 configured as an 802.1q trunk (VLAN 1) Switch 2 has ports 1-12 on VLAN 1 Switch 2 has ports 13-23 on VLAN 2 Switch 2 has port 24 configured as an 802.1q trunk (VLAN 1) Machine 1 is on port 1, switch 1. Machine 2 is on port 13, switch 2. We can send 802.1q frames with the following details... Source MAC = Machine 1 Destination MAC = Machine 2 VLAN ID = VLAN 2 ...from machine 1 and they will arrive at machine 2. This will only occur if the trunk port belongs to the same VLAN as machine 1. * We tried this only for the trunk belonging to VLAN 1. We expect that similar results would be achieve if machine 1 and the trunk port shared VLAN 3, 4, ...
This is a problem if the following conditions are met: 1. The attacker has access to a switch port on the same VLAN as the trunk. 2. The target machine is on a different switch. 3. The attacker knows the MAC address of the target machine.
In a real-life scenario, there may also be a requirement for some layer 3 device to provide a connection from VLAN 2 back to VLAN 1.

- **Cisco Catalyst SNMP Empty UDP Packet Denial of Service**
  The Catalyst series switch is a scalable, high performance layers 2 and 3 switch manufactured by Cisco Systems. The Catalyst series ranges in size, and is designed for use in organizations sized from small business to large enterprise.
  A problem with the switch firmware could allow a Denial of Service to legitimate users of network resources. Upon booting the switch with SNMP disabled, the service does not handle normal requests. However, by sending an empty UDP packet to the SNMP port, the switch ceases operating. This problem makes it possible for a remote user to deny service to legitimate users of the switch.

- **Cisco IOS BGP Transitive Attribute Denial of Service Vulnerability**
  IOS is the firmware designed for Cisco routers. IOS is a router specific firmware designed to allow networkers the ability to configure and control Cisco routers.

  A problem in IOS can allow remote users to crash Cisco routers. Upon receiving an unrecognized transitive attribute in a BGP UPDATE message, this can cause a Cisco router using an affected version of IOS to crash.

  This problem makes it possible for a remote user to crash Cisco routers using BGP, and deny service to legitimate users.

- **Cisco IOS CHAP Authentication Vulnerabilities**
  This description was taken from the Cisco advisory (see credit):

  A serious security vulnerability exists in PPP CHAP authentication in all "classic" Cisco IOS software versions (the software used on Cisco non-switch products with product numbers greater than or equal to 1000, on the AGS/AGS+/CGS/MGS, and on the CS-500, but not on Catalyst switches or on 7xx or 9xx routers) starting with the introduction of CHAP support in release 9.1(1). The vulnerability permits attackers with appropriate skills and knowledge to completely circumvent CHAP authentication. Other PPP authentication methods are not affected. A related vulnerability exists in Cisco IOS/700 software (the software used on 7xx routers).

  A moderately sophisticated programmer with appropriate knowledge can set up an unauthorized PPP connection to any system that is running vulnerable software, and that depends on CHAP for authentication. To gain this unauthorized access, an attacker must have the following:

  - Knowledge of the details of this vulnerability

  - Access to modifiable code (generally meaning source code) for a PPP/CHAP implementation, and sufficient programming skill to make simple changes to that code. Note that such source code is widely available on the Internet.

  - A modest amount of information about the configuration of the network to be attacked, including such things as usernames and IP addresses.

  This vulnerability cannot be exploited by an attacker who is using an unmodified, properly functioning PPP/CHAP implementation; the attacker must make modifications to his or her software to exploit this vulnerability.

- **Cisco IOS Crypto Engine Accelerator Access Control List Circumvention**
  It has been reported that enabled the crypto engine accelerator on Cisco routers using access control list entries may allow access for unauthorized types of traffic. This could allow an attacker to circumvent access control list policy to gain access to network resources.

- **Cisco IOS established Access List Keyword Vulnerability**
  A vulnerability in certain version of the Cisco IOS software running in the Cisco 12000 series Gigabit Switch Routers may cause it to forward unauthorized traffic due to an error in its processing of the established keyword in an access-list statement. This vulnerability only affects Cisco Gigabit Switch Routers running Cisco IOS software release 11.2(14)GS2 through 11.2(15)GS3. The vulnerability is fixed in the release 11.2(15)GS5 and later versions. When an affected Cisco Gigabit Switch Router (GSR) executes the following command on an interface:

  access-list 101 permit tcp any any established

  the established keyword is ignored. This will cause the GSR to forward all TCP traffic for the relevant interface, contrary to the restriction intended in the access-list statement.
  This is Cisco BugID CSCdm36197.

- **Cisco IOS Extended Access List Failure Vulnerability**
  IOS is the firmware used by many Cisco network devices. In some versions of IOS 12.x (verified on 12.1(4) and reportedly other versions), certain rules in extended access control lists will not be enforced. This may allow attackers to access vulnerable network services thought to be protected by the access control lists. The reason for this behaviour is not yet known.

- **Cisco IOS ICMP Redirect Denial Of Service Vulnerability**
  IOS is the Internet Operating System, used on Cisco routers. It is distributed and maintained by Cisco. It has been reported that it is possible to cause a denial of service in some Cisco routers by sending a large amount of spoofed ICMP redirect messages. This vulnerability has been assigned Cisco bug ID CSCdx32056. The following products are known to be affected:
  Cisco 1005 running IOS 11.0(18)
  Cisco 1603 running IOS 11.3(11b)
  Cisco 1603 running IOS 12.0(3)
  Cisco 2503 running IOS 11.0(22a)
  Cisco 2503 running IOS 11.1(24a)

- **Cisco IOS Malformed IKE Packet Remote Denial Of Service Vulnerability**
  Cisco IOS has been reported prone to a remote denial of service vulnerability. It is reported that the issue will present itself when IOS is running on a Cisco Catalyst 6500 Series Switch or a Cisco 7600 Series Router that has a VPN Services Module (VPNSM) installed. When one of the aforementioned appliances processes a malformed IKE packet, IOS will crash and reload.

- **Cisco IOS MSFC2 Malformed Layer 2 Frame Denial Of Service Vulnerability**
  A problem has been identified in the handling of specific types of traffic by Cisco 6000, 6500, and 7600 routers with the MSFC2 device. Because of this, an attacker could potentially crash a vulnerable system.

- **Cisco IOS Remote Router Crash**
  This description has been taken from the Cisco advisory (see credits):
  An error in Cisco IOS software makes it possible for untrusted, unauthenticated users who can gain access to the login prompt of a router or other Cisco IOS device, via any means, to cause that device to crash and reload.

  If attackers know the details of the Cisco IOS software error they will be able to cause the router to crash and reload without having to log in to the router. Because this problem involves damage to an internal data struture, it is possible that other, more subtle or targeted effects on system operation could also be induced by proper exploitation. Such exploitation, if it is possible at all, would require significant engineering skill and a thorough knowledge of the internal operation of Cisco IOS software, including Cisco trade secret information.

- **Cisco IOS RST-ACK Packet Access Control Bypass Vulnerability**
  Cisco IOS 11.2 has been reported prone to an access control bypass vulnerability. The issue is reported to present itself on C2500-F2IN-L appliances, but may also affect other Cisco devices that are running IOS 11.2. It has been repotred that an attacker who resides on a blocked network segment may bypass the access controls by transmitting TCP packets to target hosts that have both RST and ACK flags set.

- **Cisco IOS Software "?/" HTTP Request DoS Vulnerability**
  Cisco devices running IOS software may be prone to a denial of service attack if a URL containing a question mark followed by a slash (?/) is requested. The device will enter an infinite loop when supplied with a URL containing a "?/" and an enable password. Subsequently, the router will crash in two minutes after the watchdog timer has expired and will then reload. In certain cases, the device will not reload and a restart would be required in order to regain normal functionality. This vulnerability is restricted to devices that do not have the enable password set or if the password is known or can be easily predicted. The vulnerable service is only on by default in the Cisco 1003, 1004 and 1005 routers. To determine whether or not your device may be affected, log onto the device and issue the command 'show version'. If "Internetwork Operating System Software" or "IOS (tm)" and a version number appears, then IOS software is running on the system.

Cisco devices that may be running with affected IOS software releases include:

* Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, ubr900, 1000, 1400, 1500, 1600, 1700, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200, ubr7200, 7500, and 12000 series.
* Most recent versions of the LS1010 ATM switch.
* The Catalyst 6000 if it is running IOS.
* The Catalyst 2900XL LAN switch only if it is running IOS.
* The Cisco DistributedDirector.

- **Cisco IOS Software Input Access List Leakage with NAT**
  This description has been taken from the Cisco advisory:
  A group of related software bugs create an undesired interaction between network address translation (NAT) and input access list processing in certain Cisco routers running 12.0-based versions of Cisco IOS software (including 12.0, 12.0S, and 12.0T, in all versions up to, but not including, 12.0(4), 12(4)S, and 12.0(4)T, as well as other 12.0 releases). Non-12.0 releases are not affected. This may cause input access list filters to "leak" packets in certain NAT configurations, creating a security exposure. Configurations without NAT are not affected. The severity of the impact may vary, depending on the device type, configuration and environment, from sporadic leakage of occasional packets to consistent leakage of significant classes of packets. The environment dependencies are extremely complex and difficult to characterize, but essentially all vulnerable configurations are affected to some degree. Customers with affected devices are advised to assume that the vulnerability affects their networks whenever input access lists are used together with NAT in 12.0-based software. This vulnerability may allow users to circumvent network security filters, and therefore security policies. This may happen with no special effort on the part of the user, and indeed without the user being aware that a filter exists at all. No particular tools, skills, or knowledge are needed for such opportunistic attacks. In some configurations, it may be also possible for an attacker to deliberately create the conditions for this failure; doing this would require detailed knowledge and a degree of sophistication. The conditions that trigger this vulnerability may be frequent and long-lasting in some production configurations.

- **Cisco IOS Software TELNET Option Handling Vulnerability**
  Certain versions of Cisco's IOS software have a vulnerability in the Telnet Environment handling code. In particular if a certain option (ENVIRON) is passed to the Cisco IOS Telnet Daemon it will cause IOS to reload itself thereby rebooting the device it is bootstrapped on. This attack can be launched repeatedly thereby effecting a Denial of Service attack.

- **Cisco IOS Syslog Crash**
  By sending a UDP packet to the syslog port (514) of a Cisco device running classic IOS, the system can be either crashed and caused to reload or caused to hang. When it is caused to hang it will need a manual reset to recover. Specifically the tool Nmap has been known to cause such behaviour. Cisco devices that run classic Cisco IOS software include:
  - Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 8xx, ubr9xx, 1xxx, 25xx, 26xx, 30xx, 36xx, 38xx, 40xx, 45xx, 47xx, AS52xx, AS53xx, AS58xx, 64xx, 70xx, 72xx (including the ubr72xx), 75xx, and 12xxx series.
  - Most recent versions of the LS1010 ATM switch.
  - Some versions of the Catalyst 2900XL LAN switch.
  - The Cisco DitributedDirector.

- **Cisco IOS tacacs Access List Keyword Vulnerability**
  This description has been taken from the Cisco advisory. A bug in certain versions of IOS can cause extended IP access lists to be parsed incorrectly. Under some circumstances, this may allow packets to bypass IP packet filtering. This may permit unintended IP traffic to pass through a filtering router. IP extended access lists between versions 10.3(1) through 10.3(3.3) used the keyword 'tacacs-ds'. This keyword could be saved as part of the router configuration either in non-volatile memory on the router or on an external TFTP server. Configuration files written by these versions which are read by versions 10.3(3.4) through 10.3(4.2) will not have the 'tacacs-ds' keyword parsed correctly. The result will be that the entire line in the access list will be ignored. An error message will be generated when this occurs. Loss of such a line from the access list may create a vulnerability if the access list is used as part of a packet filter.

Security Update 18

Symantec NetRecon 3.6 Security Update 18 (SU 18) detects and reports 9 new vulnerabilities and provides enhanced detection of 5 vulnerabilities.

New Vulnerability detection

- **Microsoft Windows RPCSS Multi-thread Race Condition Vulnerability**
  It has been reported that a variant attack in the RPCSS service of Microsoft Windows exists. Because of this, it may be possible for an attacker to mount denial of service attacks and execute arbitrary code on the affected system. The source of the issue is reportedly a multi-thread race condition that occurs when handling a large number of RPC request.
  It has been confirmed by the vendor that this issue may be leveraged to execute arbitrary code on the affected system. This may allow an attacker to gain control of the affected system.

- **Microsoft Windows RPCSS Service Remote Denial Of Service Vulnerability**
  It has been reported that a denial of service condition exists in the RPCSS service. This issue is due to a failure of the application to properly handle malformed network messages.
  Successful exploitation of this issue may allow a remote attacker to cause the affected server to crash or stop responding. On Microsoft Windows 2000, XP and Server 2003 this will cause the affected system to reboot, on all other Windows platforms the system will have to be manually rebooted. It is currently not known whether this issue could be leveraged to execute arbitrary code on the affected system.

- **Microsoft Windows COM Internet Service/RPC Over HTTP Remote Denial Of Service Vulnerability**
  It has been reported that a denial of service condition exists in the COM Internet Service and RPC over HTTP services. This issue is due to a failure of the services to properly handle malformed network responses.
  Successful exploitation of this issue may allow a remote attacker to cause the affected server to crash or stop responding. It is currently not known whether this issue could be leveraged to execute arbitrary code on the affected system.

- **Microsoft Windows Object Identity Network Communication Vulnerability**
  It has been reported that Microsoft Windows is prone to a vulnerability in the method of creation of object identities that may allow unauthorized network communication. This issue is due to a design error that causes the process to be carried out insecurely. This issue may be leveraged by a local

attacker to open unauthorized network ports on the affected system. This may facilitate remote attacks against the affected system. There may also be other consequences.

- **Cisco IOS HTTP %% Vulnerability**
  A denial of service attack exists in versions of Cisco IOS, running on a variety of different router hardware. If the router is configured to have a web server running for configuration and other information a user can cause the router to crash.

- **Cisco Catalyst 3500 XL Remote Arbitrary Command Execution Vulnerability**
  A vulnerability exists in the webserver configuration interface which will allow an anonymous user to execute commands. A http request which includes /exec and a known filename will reveal the contents of the particular file. In addition to disclosing the contents of files, this vulnerability could allow a user to execute arbitrary code.

- **Cisco IOS HTTP Router Management Service Malformed Request Denial Of Service Vulnerability**
  The HTTP router management service on Cisco IOS has been reported to be prone to a remote denial of service vulnerability. On Cisco IOS versions 12.0T and up, the "?" character when appended with a "/" character is not properly interpreted by the HTTP router management service and may cause the appliance to crash.

- **Cisco Context Based Access Control Protocol Check Bypassing Vulnerability**
  IOS is a Cisco Internetwork Operating System. It is maintained and distributed by Cisco, and used on various types of Cisco hardware.

  A problem has been found in the checking of protocol by the system. The vulnerable version of IOS does not check the protocol type of the packets, thus making it possible for a system on either end of the connection to send data of a different type. One such instance would be a system on the protected network sending a UDP packet to a system outside of the protected network, and the external system returning a connection to the host via TCP using the pre-established IP address and port numbers. This could allow a remote user to gather intelligence about a host, and potentially lead to an organized attack against network resources.

- **Microsoft Windows Help And Support Center URI Validation Code Execution Vulnerability**
  Microsoft has reported a vulnerability in the Help and Support Center that is related to how HCP URIs are validated. This issue could reportedly be

exploited via a malicious web page or HTML e-mail to execute arbitrary code on a client system.

The issue may permit an attacker to inject invocation arguments when HCP URIs cause the HelpCtr.exe component to be executed. By placing malicious content into a known location on the system, whose contents the attacker may influence via a malicious web page, it is possible to exploit this issue to cause the malicious content to be executed in the Local Zone.

It should be noted that the vulnerable functionality is included in Microsoft Windows ME but that the vendor has not considered this vulnerability to pose a serious threat to users of this operating system. The vendor has not qualified why the threat is reduced for Windows ME users.

Enhanced vulnerability detection

- **Microsoft Internet Explorer MHTML Forced File Execution Vulnerability**
  A vulnerability has been discovered in Outlook Express when handling MHTML file and res URIs that could lead to an unexpected file being downloaded and executed. The problem occurs due to the component failing to securely handle MHTML file URIs that reference a non-existent resource. The affected Outlook Express component is used by Microsoft Internet Explorer. As a result, a victim browser user may inadvertently access a page designed to load an embedded object from a malicious location. This would effectively result in the execution of attacker-supplied code within the Local Zone. The vulnerability is present even if Microsoft Outlook has been removed as the default e-mail client.

Note: Microsoft Internet Explorer on Windows Server 2003 is vulnerable despite its specialized configuration.

Note: Now considers patch KB837009 before reporting.

- **Microsoft Internet Explorer Browser MHTML Redirection Local File Parsing**
  The issue is reported to present itself if the resource specified in the Mhtml_File_Uri cannot be found, the browser will attempt to retrieve the resource specified in the Original_Resource_Uri. Due to insufficient security checks when accessing the Original_Resource_Uri, it is possible to use this to redirect the browser to a local resource.
  This issue was originally covered in BID 9100 "Multiple Internet Explorer Browser Security Model Compromise Vulnerabilities" and is now being assigned

its own BID. MHTML is a component of Outlook Express but may be accessed via Internet Explorer.

Note: Now considers patch KB837009 before reporting

- **Microsoft IE Invalid ContentType Cache Directory Location Disclosure**
  Microsoft Internet Explorer is prone to a weakness that may allow attackers to enumerate where cached Internet content is stored on the client filesystem. The attacker can exploit this by specifying an invalid ContentType in an HTTP response to the browser. If the attacker can determine the location of cached content, it may be possible to reference this content using other known issues and cause it to be executed. This could be exploited in tandem with other vulnerabilities from a malicious web page to cause code to be executed on a vulnerable client system.

Note: Now considers patch KB837009 before reporting

- **Microsoft IE File Download Warning Bypass Vulnerability**
  It has been reported that Microsoft Internet Explorer may be prone to a vulnerability when handling file URIs that may be exploited to download a malicious file to the client system. It has been reported that by renaming a file, an attacker may be able to trick the browser, bypassing the security warning. An attacker may name a file in the following format to conceal the extension type from the browser: http://www.example.com/file.exe?.html. Successful exploitation of this issue may allow an attacker to plant malicious files on vulnerable systems in order to execute malicious code. This issue has reportedly been tested with Microsoft Internet Explorer running on a Windows 2003 Web Server edition platform, however, other versions are likely to be affected as well.

Note: Now considers patch KB810847 before reporting

- **Microsoft Internet Explorer MT-ITS Protocol Zone Bypass Vulnerability**
  Microsoft Internet Explorer has been reported prone to a vulnerability that may permit hostile content to be interpreted in the Local Zone. The issue may be exploited via the ITS (InfoTech Storage) Protocol URI handler. It is possible to use this protocol to force a browser into the Local Zone by redirecting into a non-existent MHTML file (using other known vulnerabilities). In this manner, it may be possible to reference hostile content to be executed in the Local Zone, such as a malicious CHM file. The issue, in combination with other vulnerabilities, is exploitable to provide for automatic delivery and execution of an arbitrary executable. This would

occur when malicious web content is rendered in Internet Explorer. Outlook products and other components that use Internet Explorer to render HTML content also present possible attack vectors for this issue. Note that there are multiple ways to invoke the protocol handler, such as through its:, ms-its:, ms-itss: and mk:@MSITStore: URIs. It has also been reported that web browsers other than Internet Explorer may also invoke the operating system URI handlers for the ITS protocol.

It has been reported that this vulnerability is actively being exploited as an infection vector for malicious code that has been dubbed Trojan.Ibiza.

Note: Microsoft has released a cumulative update for Outlook Express (MS04-013) to address the MHTML-related vulnerabilities that are commonly exploited in tandem with this issue. While MS04-013 lists the same CVE candidate name as this BID, it is not currently known if this update also addresses the distinct ITS Protocol vulnerability. However, users are advised to apply the available updates, as they will reduce exposure to existing exploits that rely on the MHTML issues to exploit this or other vulnerabilities. If this individual vulnerability has not been addressed by the update, there may still potentially be other attack vectors which do not rely on the MHTML issues.

Note: Now considers patch KB837009 before reporting

Security Update 17

Symantec NetRecon 3.6 Security Update 17 (SU 17) enhances detection of one vulnerability.

- **Microsoft Windows LSASS Buffer Overrun Vulnerability**
  Microsoft Windows LSASS (Local Security Authority Subsystem Service) is prone to a remotely exploitable buffer overrun vulnerability. The specific vulnerable system component is LSASRV.DLL. Successful exploitation of this issue could allow a remote attacker to execute malicious code on a vulnerable system, resulting in full system compromise.

  This issue could be exploited by an anonymous user on Microsoft Windows 2000 and XP operating systems. The issue may reportedly only be exploited by local, authenticated users on Microsoft Windows Server 2003 and Microsoft Windows XP 64-Bit Edition 2003. Microsoft has stated that a local administrator could exploit the issue on these platforms, though this does not appear to pose any additional security risk as the administrator will likely already have complete control over the system.

An exploit for this vulnerability has been incorporated into the Sasser family of worms.

Security Update 16

Symantec NetRecon 3.6 Security Update 16 (SU 16) detects and reports fifteen additional vulnerabilities.

New vulnerability detection

- **Apache Cygwin Directory Traversal Vulnerability**
  It has been reported that Apache may be prone to a directory traversal vulnerability that may allow a remote attacker to access information outside the server root directory. This issue is only reported to present itself in Apache running on cygwin platforms. A remote attacker may traverse outside the server root directory by using encoded '\..' character sequences.
- **Apache Error Log Escape Sequence Injection Vulnerability**
  It has been reported that the Apache web server is prone to a remote error log escape sequence injection vulnerability. This issue is due to an input validation error that may allow escape character sequences to be injected into apache log files. This may facilitate exploitation of issues such as those found in BIDs 6936 and 6938. This issue may allow an attacker to carry out a number of actions including arbitrary file creation and code execution on the affected system.
- **Apache Mod_Access Access Control Rule Bypass Vulnerability**
  Apache mod_access has been reported to be prone to an access rule bypass vulnerability. When an Allow or Deny rule is specified and an IP address is used in the rule without a netmask, the affected module may fail to match the rule. As a result of this vulnerability, access controls may not be enforced correctly.
- **Apache mod_disk_cache Module Client Authentication Credential Storage Weakness**
  It has been reported that Apache mod_disk_cache module may be prone to a weakness that could result in an attacker gaining access to proxy or standard authentication credentials. The mod_disk_cache module is reported to store HTTP Hop-by-hop headers including user login and password information in plaintext format on disk. This issue could be used in conjunction with other possible vulnerabilities in a host to gain access to user authentication credentials. Successful exploitation of this issue may lead to further attacks against vulnerable users of the affected host. Apache versions 2.0.49 and prior with mod_disk_cache enabled are assumed to be affected by this issue.

- **Apache Mod_SSL HTTP Request Remote Denial Of Service Vulnerability**
  mod_ssl has been reported to be prone to a remote denial of service vulnerability. It has been reported that the issue is as a result of a memory leak and will present itself when standard HTTP requests are handled on the SSL port of an affected Apache server.
- **Foxmail Remote Buffer Overflow Vulnerability**
  It has been reported that Foxmail is prone to a remote buffer overflow vulnerability. This issue is due to a failure of the application to verify buffer boundaries when processing user supplied email headers. A remote attacker may potentially exploit this issue to cause the email client to crash, denying service to the victim user. It is also possible to further leverage this issue in order to execute arbitrary code; this code would be executed in the security context of the user running the affected email client.
- **Ipswitch WS_FTP Multiple Vulnerabilities**
  Multiple vulnerabilities have been identified in the WS_FTP Server and client applications. These vulnerabilities may allow remote attackers to execute arbitrary code, cause denial of service attacks and gain administrative level access to a server. The issues include two remote buffer overflow vulnerabilities in the client, a denial of service vulnerability in the server and an access validation issue in the server leading to remote command execution with SYSTEM privileges. These issues are undergoing further analysis. This BID will be divided into separate issues as analysis is completed.
- **Jet Database Engine command interpretation allows remote code execution**
  Microsoft's Jet Database Engine (Jet) is vulnerable to a buffer overflow attack that may grant remote attackers system level privileges. Elevated access of this type allows intruders to perform any system task including interfering with running services, modifying user access including creating new accounts, deleting and creating files, as well as running applications both stored on the system and those copied to the system by the remote intruder. All information stored on the vulnerable system may be compromised. By failing to properly handle Jet database commands, the Jet Database Engine is vulnerable to buffer overflow attacks that may execute arbitrary code. The Jet Database Engine is included in Microsoft Windows 2000, XP, and Server 2003. Windows NT 4.0 could be vulnerable if the Jet Engine has been installed. Many applications use the Jet engine. IIS servers are particularly vulnerable as IIS uses the Jet Database to process some web requests. Because IIS is often used as a World Wide Web server this exposes the vulnerability to the public.

- **Kerio MailServer Spam Filter Buffer Overrun Vulnerability**
  Kerio has reported that MailServer is prone to a remotely exploitable buffer overrun condition. This vulnerability exists in the spam filter component. If successfully exploited, this could permit remote attackers to execute arbitrary code in the context of the MailServer software. This could also cause a denial of service in the server.
- **Microsoft Internet Explorer MT-ITS Protocol Zone Bypass Vulnerability**
  Microsoft Internet Explorer has been reported prone to a vulnerability that may permit hostile content to be interpreted in the Local Zone. The issue may be exploited via the ITS (InfoTech Storage) Protocol URI handler. It is possible to use this protocol to force a browser into the Local Zone by redirecting into a non-existent MHTML file (using other known vulnerabilities). In this manner, it may be possible to reference hostile content to be executed in the Local Zone, such as a malicious CHM file. The issue, in combination with other vulnerabilities, is exploitable to provide for automatic delivery and execution of an arbitrary executable. This would occur when malicious web content is rendered in Internet Explorer. Outlook products and other components that use Internet Explorer to render HTML content also present possible attack vectors for this issue. It should be noted that there are multiple ways to invoke the protocol handler, such as through its:, ms-its:, ms-itss: and mk:@MSITStore: URIs. It has also been reported that web browsers other than Internet Explorer may also invoke the operating system URI handlers for the ITS protocol. It has been reported that this vulnerability is actively being exploited as an infection vector for malicious code that has been dubbed Trojan.Ibiza.
- **Microsoft Internet Explorer window.open Search Pane Cross-Zone Scripting**
  A vulnerability has been reported in Microsoft Internet Explorer that could enable unauthorized access by malicious scripts and Active Content to document properties across different Security Zones and foreign domains. This issue is exposed when search panes are opened via the window.open method. It is possible for malicious script code to access the properties of a foreign domain opened within the search pane. Exploitation of this issue could allow various attacks, such as cookie-theft from an arbitrary domain. Other issues, such as additional described in BID 8577, may also facilitate execution of arbitrary code on a vulnerable client system. It should be noted that support for the search pane was introduced in Internet Explorer 5. This issue was originally described in BID 8577 "Multiple Microsoft Internet Explorer Script Execution Vulnerabilities".
- **ProFTPD _xlate_ascii_write() Buffer Overrun Vulnerability**
  A remotely exploitable buffer overrun was reported in ProFTPD. This issue is due to insufficient bounds checking of user-supplied data in the

_xlate_ascii_write() function, permitting an attacker to overwrite two bytes memory adjacent to the affected buffer. This may potentially be exploited to execute arbitrary code in the context of the server. This issue may be triggered when submitting a RETR command to the server.

- **Sun Solaris vfs_getvfssw function Local Privilege Escalation Vulnerability**
  A remotely exploitable buffer overrun was reported in ProFTPD. This issue is due to insufficient bounds checking of user-supplied data in the _xlate_ascii_write() function, permitting an attacker to overwrite two bytes memory adjacent to the affected buffer. This may potentially be exploited to execute arbitrary code in the context of the server. This issue may be triggered when submitting a RETR command to the server.

- **Windows NtSystemDebugControl() Kernel API Function Privilege Escalation**
  It has been reported that security exposures exist in kernel API functions for Microsoft Windows operating systems that may permit local privilege escalation attacks. These issues were reported to exist in Microsoft Windows XP but it has been conjectured that Microsoft Windows Server 2003 may also be affected by these issues. It should be noted that a local user would require the SeDebugPrivilege to exploit these issues.

- **WU-FTPD restricted-gid Unauthorized Access Vulnerability**
  It has been reported that WU-FTPD FTP server is prone to an unauthorized access vulnerability. The issue is related to the "restricted-gid" feature supported by WU-FTPD. This feature allows for an administrator to restrict FTP user access to certain directories. The vulnerability reportedly allows users to bypass those restrictions through modifying the permissions on their home directory so that they themselves can no longer access it. Under such circumstances, the server may grant the user unauthorized access to the root directory. Further technical details are not known at this time. This record will be updated as more information becomes available. This BID is created in response to Two Possibly New WU-FTPD Vulnerabilities BID 9820. BID 9820 is being retired.

Security Update 15

Symantec NetRecon 3.6 Security Update 15 (SU 15) detects and reports five additional vulnerabilities. Symantec NetRecon 3.6 Security Update 15(SU 15) includes enhanced detection and reporting of four vulnerabilities.

New vulnerability detection

- **Microsoft MSN Messenger Information Disclosure Vulnerability**
  Microsoft MSN Messenger is prone to an information disclosure vulnerability. When a malformed file transfer request is initiated by a remote user, they may be able to view the contents of files on the remote system.
- **Microsoft Windows Media Services Remote Denial of Service Vulnerability**
  It has been reported that Microsoft Windows Media Services is prone to a remote denial of service vulnerability. This may allow an attacker to cause the services to effectively deny access to legitimate users by sending specially crafted TCP/IP packets on TCP ports 7007 and/or 7778.
  Microsoft Windows Media Services 4.1 included with Microsoft Windows 2000 Server Service Pack 2, Service Pack 3, and Service Pack 4 is reported to be vulnerable to this issue. Windows Media Services 4.1 for Windows NT 4.0 is not vulnerable.
- **Windows Media Services MX_STATS_LogLine NSIISlog.DLL Remote Buffer Overflow Vulnerability**
  Microsoft Media Services has been reported prone to a buffer overflow vulnerability. This is due to a problem with how the logging ISAPI extension handles incoming client MX_STATS_LogLine: header field data in POST requests. The logging facility may attempt to write excessive data to an undersized buffer when handling a malformed HTTP client request. This could trigger a denial of service or remote arbitrary code execution in IIS, which is exploitable through Media Services.
- **Microsoft Windows XP explorer.exe Remote Denial of Service Vulnerability**
  It has been reported that Windows Explorer for Windows XP may be prone to a denial of service vulnerability that may allow a remote attacker to cause the system to hang by sending a malicious directory containing 'wmf' files to a vulnerable user via e-mail or other means. Windows Explorer automatically attempts to parse 'wmf' files in the directory, however, an exceptional condition occurs if the directory contains records of zero length. Although unconfirmed, all versions of Windows XP are considered to be affected by this vulnerability.

- **Multiple Vendor Internet Browser Cookie Path Argument Restriction Bypass Vulnerability**
  Multiple vendor Internet Browsers have been reported to be prone to a cookie path argument restriction bypass vulnerability. The issue presents itself due to a failure to properly sanitize encoded URI content. This may make it possible for an attacker to craft a URI that will contain encoded directory traversal sequences sufficient to provide access to a supposedly path exclusive cookie from an alternate path.

Enhanced vulnerability detection

- **Microsoft Internet Explorer BackToFramedJPU Cross-Domain Policy Vulnerability**
  A vulnerability has been in sub-frames in Microsoft Internet Explorer. Because of this, an attacker may be able to violate cross-domain policy. This could permit script code to access properties of other domains or execute in the context of the Local Zone. Exploitation of this issue in combination with other vulnerabilities could allow for execution of a malicious executable on a vulnerable system.
- **Multiple Browser URI Display Obfuscation Weakness**
  A weakness has been reported in multiple browsers that may allow attackers to obfuscate the URI for a visited page. The problem is said to occur when a URI designed to pass access a specific location with a supplied username, contains a hexadecimal 1 value prior to the @ symbol. An attacker could exploit this issue by supplying a malicious URI pointing to a page designed to mimic that of a trusted site, and tricking a victim who follows a link into believing they are actually at the trusted location.
- **Apache Web Server MIME Boundary Information Disclosure Vulnerability**
  A vulnerability has been discovered in the Apache web server that may result in the disclosure of sensitive information. Specifically, sensitive process information is used within generated MIME message boundaries. Access to this information may aid an attacker in launching attacks further attacks against target services. OpenBSD has released a patch that addresses this issue. MIME boundaries are now generated by the server using BASE64 encoded random numbers.

Security Update 14

Symantec NetRecon 3.6 Security Update 14 (SU 14) detects and reports eleven additional vulnerabilities.

New vulnerability detection

- **PHP HTTP POST Incorrect MIME Header Parsing Vulnerability**
  A vulnerability has been reported for PHP versions 4.2.0 and 4.2.1. It is possible for a remote attacker to cause the PHP interpreter to crash the web server on a vulnerable system and execute malicious, attacker supplied code. The vulnerability is the result of the PHP interpreter incorrectly parsing MIME headers when HTTP POST commands are received. When PHP receives a malformed POST request, it generates an error condition that is improperly handled. As a result, the attacker may cause the Web server to crash and possibly execute supplied code.
- **Apache Web Server mod_cgid Module CGI Data Redirection Vulnerability**
  Apache has reported a vulnerability in the mod_cgid module when the threaded MPM is used. The problem is said to occur due to mishandling of CGI redirect paths. The condition may potentially cause CGI data to inadvertently be sent to the wrong client. Depending on the context of the data being redirected, this could potentially expose sensitive information or incorrectly grant unauthorized access.
- **Apache Web Server Multiple Module Local Buffer Overflow Vulnerability**
  A vulnerability has been reported in Apache that could allow a local attacker execute arbitrary code on a vulnerable host computer. The issue is reported to exist due to a lack of bounds checking by the software, leading to a buffer overflow condition. The problem is reported to exist in the mod_alias and mod_rewrite modules when a regular expression is configured with more the nine captures using parentheses. This issue could let an attacker gain unauthorized access to a vulnerable host. Successful exploitation of this vulnerability could allow an attacker execute arbitrary code in the context of the Web server to gain unauthorized access to a vulnerable computer.
- **Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability**
  IOS is router firmware developed and distributed by Cisco Systems. IOS functions on numerous Cisco devices, including routers and switches. It is possible to gain full remote administrative access on devices using affected releases of IOS. By using a URL of http://router.address/level/$NUMBER/exec/... where $NUMBER is an integer between 16 and 99, it is possible for a remote user to gain full administrative access. This problem makes it

possible for a remote user to gain full administrative privileges, which may lead to further compromise of the network or result in a denial of service.

- **Cisco CatOS Password Prompt Unauthorized Remote Command Execution Vulnerability**
  It has been alleged that it is possible for remote attackers to execute arbitrary commands without proper authorization. Reportedly it is possible to execute shell commands from the password prompt on a device running a vulnerable version of CatOS. This issue has been reported in CatOS versions 5.4(2) and 5.5(2) on Cisco Catalyst 6509 switches. Other devices and CatOS versions may also be similarly affected. Cisco has replied to this issue stating that it cannot be used to execute commands, retrieve information from the device, or reveal information about traffic processed by the device. Details are available to registered Cisco users at: http://www.cisco.com/pcgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdr87435. Since this issue cannot be exploited to compromise any security properties on the device, this BID will be retired.
- **Cisco IOS UDP Denial of Service Vulnerability**
  A potential denial of service condition may exist in Cisco's IOS firmware. The problem reportedly occurs when a large number of UDP packets is sent to a device running IOS. This causes the system to use all available CPU resources and thus become unresponsive. The device may have to be reset manually if the attack is successful.
- **Multiple Vendor SSH2 Implementation Buffer Overflow Vulnerabilities**
  Multiple vendor SSH2 implementations are reported to be prone to buffer overflows. These buffer overflows are alleged to be exploitable prior to authentication.

  These conditions were discovered during tests of the initialization, key exchange, and negotiation phases (KEX, KEXINIT) of a SSH2 transaction between client and server. These issues are known to affect various client and server implementations of the protocol. Successful exploitation will enable remote attackers to cause execution of code in the security context of the specific server and client implementations. Further details about this vulnerability are currently unknown. This BID will be updated as more information becomes available. This vulnerability was originally described in BugTraq ID 6397.
- **Cisco Aironet Access Point Wired Equivalent Privacy Key Disclosure Vulnerability**
  Cisco Aironet Access Points that are running Cisco IOS have been reported prone to an information disclosure vulnerability that could lead to the disclosure of wired equivalent privacy (WEP) keys. The issue has been reported to exist if the snmp-server enable traps wlan-wep command has

been set. The issue presents itself because, when this functionality is enabled, the Cisco Aironet Access Point will send the WEP key in a plain text format to the simple network management protocol server.

- **Microsoft Windows Internet Naming Service Buffer Overflow Vulnerability**
  The Microsoft Windows Internet Name Service (WINS) is prone to a remotely exploitable buffer overflow condition. Sending a series of specially crafted packets to the service could cause it to fail. On some Windows platforms, this could also lead to execution of arbitrary code.

- **Microsoft ASN.1 Library Length Integer Mishandling Memory Corruption Vulnerability**
  vulnerability has been reported in the Microsoft ASN.1 library. This issue is related to insufficient checking of data supplied via an externally supplied length field in ASN.1 BER encoded data. This could result in an excessive value being used in a heap allocation routine, allowing for large amounts of heap memory to be corrupted. This could be leveraged to corrupt sensitive values in memory, resulting in execution of arbitrary code. This vulnerability is exposed in a number of security related operating system components, including Kerberos (via UDP port 88), Microsoft IIS with SSL support enabled and NTLMv2 authentication (via TCP ports 135, 139 and 445). Other components may also be affected, though a comprehensive list is not available at this time. It should be noted that because ASN.1 data will likely be encoded, for example Kerberos, SSL, IPSec or Base64 encoded, the malicious integer values may be obfuscated and as a result not easily detectable.

- **Microsoft Windows ASN.1 Library Bit String Processing Integer Handling Vulnerability**
  Microsoft ASN.1 handling library has been reported prone to an integer overflow vulnerability that may result in arbitrary heap-based memory corruption. The issue presents itself in the ASN.1 BER decoding/encoding routines. Exploitation of this issue will result in the corruption of heap based management structures, and may ultimately be leveraged by an attacker to have arbitrary code executed in the context of the affected process. This vulnerability is exposed in a number of security related operating system components, including Kerberos (via UDP port 88), Microsoft IIS with SSL support enabled and NTLMv2 authentication (via TCP ports 135, 139 and 445). Other components may also be affected, though a comprehensive list is not available at this time. It should be noted that because ASN.1 data will likely be encoded, for example Kerberos, SSL, IPSec or Base64 encoded, the malicious integer values may be obfuscated and as a result not easily detectable.

Security Update 13

Symantec NetRecon 3.6 Security Update 13 (SU 13) detects and reports eleven additional vulnerabilities.

New vulnerability detection

- **Multiple Vendor Telnetd Buffer Overflow Vulnerability**
  A boundary condition error exists in telnet daemons derived from the BSD telnet daemon. Under certain circumstances, the buffer overflow can occur when a combination of telnet protocol options are received by the daemon. The function responsible for processing the options prepares a response within a fixed sized buffer, without performing any bounds checking. This vulnerability is now being actively exploited. A worm is known to be circulating around the Internet.
- **OpenSSL ASN.1 Parsing Vulnerabilities**
  Multiple vulnerabilities were reported in the ASN.1 parsing code in OpenSSL. These issues could be exploited to cause a denial of service or to execute arbitrary code.
- **Cisco Discovery Protocol Neighbor Announcment Denial of Service Vulnerability**
  Cisco Discovery Protocol (CDP) is a network neighbor discovery protocol distributed with implementations of the Cisco Internet Operating System. CDP is implemented with some releases of the Cisco Internet Operating System. It is possible for a host on a local segment of network to cause a Cisco router to become unstable, and potentially stop routing traffic by generating large amounts of CDP traffic. This protocol can not be routed across routers to remote network segments. This could lead to the ceasing of operation of Cisco routers, and a denial of service.
- **Cisco IOS TFTP Server Long File Name Buffer Overflow Vulnerability**
  A problem has been discovered in Cisco IOS and MGX switches that could result in a denial of service, and potential code execution. It has been discovered that the TFTP server file name handling of Cisco IOS is vulnerable to a buffer overflow. This overflow results due insufficient bounds checking on requested file names. A request for a file name of 700 or more bytes will result a crash of the router, and reboot of the device. On Cisco MGX switches, the TFTP service will fail but the device will continue to function. Cisco IOS versions 12.0 and later are not prone to this issue. Cisco has assigned Cisco Bug ID CSCdy03429 to this vulnerability. Cisco has announced that some MGX switches are also affected by this issue. Cisco has assigned Cisco Bug ID CSCdy03429 to this vulnerability.

- **Cisco IOS ILMI SNMP Community String Vulnerability**
  IOS is the operating system designed for various Cisco devices. It is maintained and distributed by Cisco systems. A problem in the versions of IOS 11.x and 12.0 could allow unauthorized access to certain configuration variables within a Cisco device. The ILMI SNMP Community string allows read and write access to system objects in the MIB-II community group. These configuration parameters do not affect the normal operation of the device, although if changed, can cause confusion or lead to a social engineering attack. It is possible for a malicious remote user to change configuration objects within the MIB-II Community, and rename the system, change the location name in the system, and/or the contact information for the system. This vulnerability affects only certain devices.
- **Oracle Database Server ORACLE.EXE Buffer Overflow Vulnerability**
  The 'ORACLE.EXE' binary does not implement sufficient bounds checking on external data which is copied into local memory buffers. An attacker may exploit this problem to corrupt sensitive regions of memory, in an effort to execute arbitrary code. Code will be executed with the privileges of the underlying server. This issue may only be exploited if a client application does not place bounds limits on externally supplied data before passing it to Oracle.
- **Microsoft Exchange Server Buffer Overflow Vulnerability**
  Microsoft has announced that Exchange Server is affected by a remotely exploitable buffer overflow condition. The overflow can be triggered remotely by unauthenticated SMTP clients. The source of the issue appears to be in how the XEXCH50 verb is handled by the server. Microsoft has stated that remote code execution is possible on hosts running Exchange 2000 Server. Servers running Exchange Server 5.5 are vulnerable to a denial of service attack.
- **Solaris sadmind Buffer Overflow Vulnerability**
  Certain versions of Solaris ship with a version of sadmind which is vulnerable to a remotely exploitable buffer overflow attack. sadmind is the daemon used by Solstice AdminSuite applications to perform distributed system administration operations such as adding users. The sadmind daemon is started automatically by the inetd daemon whenever a request to invoke an operation is received. Under vulnerable versions of sadmind (2.6 and 7.0 have been tested), if a long buffer is passed to a NETMGT_PROC_SERVICE request (called via clnt_call()), it is possible to overwrite the stack pointer and execute arbitrary code. The actual buffer in questions appears to hold the client's domain name. The overflow in sadmind takes place in the get_auth() function, part of the /usr/snadm/lib/libmagt.so.2 library. Because sadmind runs as root any code launched as a

result will run as with root privileges, therefore resulting in a root compromise.

- **Multiple Vendor Network Device Driver Frame Padding Information Disclosure Vulnerability**
  Network device drivers for several vendors have been reported to disclose potentially sensitive information to attackers. Frames that are smaller than the minimum frame size should have the unused portion of the frame buffer padded with null (or other) bytes. Some device drivers do not do this adequately, leaving the data that was stored in the memory comprising the buffer prior to its use intact. Consequently, this data may be transmitted within frames across ethernet segments. As the ethernet frame buffer is allocated in kernel memory space, sensitive data may be leaked. Cisco has stated that the IOS 12.1 and 12.2 trains are not affected. National Semiconductor Ethernet controller chips are not vulnerable to this issue.
- **Microsoft Internet Explorer File Download Warning Bypass Vulnerability**
  It has been reported that Microsoft Internet Explorer may be prone to a vulnerability when handling file URIs that may be exploited to download a malicious file to the client system. It has been reported that by renaming a file, an attacker may be able to trick the browser, bypassing the security warning. An attacker may name a file in the following format to conceal the extension type from the browser: http://www.example.com/file.exe?.html. Successful exploitation of this issue may allow an attacker to plant malicious files on vulnerable systems in order to execute malicious code. This issue has reportedly been tested with Microsoft Internet Explorer running on a Windows 2003 Web Server edition platform, however, other versions are likely to be affected as well.
- **Multiple Browser URI Display Obfuscation Weakness**
  A weakness has been reported in multiple browsers that may allow attackers to obfuscate the URI for a visited page. The problem is said to occur when a URI designed to pass access a specific location with a supplied username, contains a hexadecimal 1 value prior to the @ symbol. An attacker could exploit this issue by supplying a malicious URI pointing to a page designed to mimic that of a trusted site, and tricking a victim who follows a link into believing they are actually at the trusted location.

Security Update 12

Symantec NetRecon 3.6 Security Update 12 (SU 12) detects and reports nine additional vulnerabilities.

New vulnerability detection

- **Microsoft Internet Explorer BackToFramedJPU Cross-Domain Policy Vulnerability**
  A vulnerability has been in sub-frames in Microsoft Internet Explorer. Because of this, an attacker may be able to violate cross-domain policy. This could permit script code to access properties of other domains or execute in the context of the Local Zone. Exploitation of this issue in combination with other vulnerabilities could allow for execution of a malicious executable on a vulnerable system.
- **Microsoft Internet Explorer MHTML Forced File Execution Vulnerability**
  A vulnerability has been discovered in Microsoft Internet Explorer when handling MHTML file and res URIs that could lead to an unexpected file being downloaded and executed. The problem occurs due to the browser failing to securely handle MHTML file URIs which references two files, the first of which points to a non-existent resource. As a result, a victim browser user may inadvertently access a page designed to load an embedded object from a malicious location. This would effectively result in the execution of attacker-supplied code within the Internet Zone.
- **Microsoft Internet Explorer Browser MHTML Redirection Local File Parsing Vulnerability**
  A vulnerability has been reported in Internet Explorer that may allow an attacker to parse local files on a system.
  The issue is reported to present itself if the resource specified in the Mhtml_File_Uri cannot be found, the browser will attempt to retrieve the resource specified in the Original_Resource_Uri. Due to insufficient security checks when accessing the Original_Resource_Uri, it is possible to use this to redirect the browser to a local resource.
- **Microsoft Internet Explorer Invalid ContentType Cache Directory Location Disclosure Weakness**
  Microsoft Internet Explorer is prone to a weakness that may allow attackers to enumerate where cached Internet content is stored on the client filesystem. The attacker can exploit this by specifying an invalid ContentType in an HTTP response to the browser. If the attacker can determine the location of cached content, it may be possible to reference this content using other known issues and cause it to be executed. This

could be exploited in tandem with other vulnerabilities from a malicious web page to cause code to be executed on a vulnerable client system.

- **Cisco IOS 2GB HTTP GET Buffer Overflow Vulnerability**
  The HTTP server on Cisco IOS devices is prone to a buffer overrun that can be triggered by sending 2GB of data. This may be exploited to execute arbitrary code on a vulnerable device.
- **Cisco IOS UDP Echo Service Memory Disclosure Vulnerability**
  It has been reported that under some circumstances, a Cisco appliance running IOS may answer malicious malformed UDP echo packets with replies that contain partial contents from the affected router's memory.
- **Cisco IOS Malicious IPV4 Packet Sequence Denial Of Service Vulnerability**
  A denial of service vulnerability has been reported to exist in all hardware platforms that run Cisco IOS versions 11.x through 12.x. This issue may be triggered by a sequence of specifically crafted IPV4 packets. A power cycling of an affected device is required to regain normal functionality.
- **Cisco Catalyst Non-Standard TCP Flags Remote Denial of Service Vulnerability**
  A problem with Cisco Catalyst switches has been reported in the handling of non-standard TCP packets. Because of this, an attacker may be able to deny legitimate user access to the switch.
- **Cisco IOS Crypto Engine Accelerator Access Control List Circumvention Vulnerability**
  It has been reported that Cisco IOS is vulnerable to an issue in handling Service Assurance Agent (previously called Response Time Reporter, or RTR) packets. Because of this, a remote user may be able to cause the router to become unstable and crash.

Security Update 11

Symantec NetRecon 3.6 Security Update 11 (SU 11) detects and reports nine additional vulnerabilities.

New vulnerability detection

- **Sendmail Headers Prescan Denial Of Service Vulnerability**
  Sendmail has been reported prone to a denial of service vulnerability when handling malicious SMTP mail headers. The vulnerability has been reported to present itself, due to an inefficient implementation of a header prescan algorithm. A remote attacker may reportedly deny service to legitimate users by sending specially crafted mails to the affected service.

- **Sendmail Ruleset Parsing Buffer Overflow Vulnerability**
  Sendmail has been reported prone to a buffer overflow condition when parsing non-standard rulesets.
  It has been reported that an attacker may trigger a buffer overflow condition in Sendmail, when sendmail parses specific rulesets. It should be noted that Sendmail under a default configuration is not vulnerable to this condition. It is not currently known, if this vulnerability may potentially be exploited to execute arbitrary code. However due to the nature of this vulnerability, although unconfirmed, it has been conjectured that ultimately an attacker may exploit this condition to execute arbitrary code in the context of the affected Sendmail server.

- **Sendmail Prescan() Variant Remote Buffer Overrun Vulnerability**
  Sendmail is prone to a buffer overrun vulnerability in the prescan() function. This issue is different than the vulnerability described in BID 7230. This vulnerability could permit remote attackers to execute arbitrary code via vulnerable versions of Sendmail.

- **Sendmail DNS Maps Remote Denial of Service Vulnerability**
  A potential vulnerability has been discovered in Sendmail 8.12.x versions prior to 8.12.9, when implementing the use of DNS Maps. The problem specifically lies in the fact that Sendmail fails to properly initialized dynamically allocated data, which may referenced at a later time when freeing memory.
  The problem specifically occurs when an invalid DNS reply is returned, specifically one with a differing size than announced. This will cause Sendmail to enter a routine designed to free the final object from a list of the uninitialized structures. The structures are traversed until a NULL pointer is detected, however due to the incorrect initialization the structures may contain garbage data, potentially triggering a call to free() on random data. This would effectively result in Sendmail dereferencing invalid data, causing it to crash.
  Theoretically, if this data were to be controlled by an attacker at some point during execution, it may be possible to exploit this issue to execute arbitrary code. This however has not been confirmed.

- **Sendmail V.5 -oR Privilege Escalation Vulnerability**
  Sendmail V.5 is prone to a privilege escalation vulnerability. This issue is due to improper handling of the -oR option (either from the command line or from a configuration file). Exploitation could permit a local attacker to gain elevated privileges.
  This issue affects Sendmail versions on SunOS 4.1.x systems, but also affects Sendmail V.5 on other Unix operating systems.

- **MySQL Multiple Vulnerabilities**
  Multiple vulnerabilities have been reported for MySQL. The precise nature of these vulnerabilities are currently unknown however, exploitation of this issue may result in an attacker obtaining unauthorized access, elevated privileges and execution of arbitrary code.
  These issue were fixed in MySQL version 3.23.54.
  These vulnerabilities may be related to known issues in MySQL (BIDs 6375, 6374, 6373, 6370, 6368), however this has not been confirmed by Symantec. This BID and any other applicable BIDs will be updated as further information is available.'

- **MySQL Password Handler Buffer Overflow Vulnerability**
  MySQL server has been reported prone to a buffer overflow vulnerability when handling user passwords of excessive size.
  The issue presents itself, due to a lack of sufficient bounds checking performed when processing MySQL user passwords. A password greater that 16 characters may overrun the bounds of a reserved buffer in memory and corrupt adjacent memory. An attacker with global administrative privileges on an affected MySQL server may potentially exploit this condition to have arbitrary supplied instructions executed in the context of the MySQL server.

- **MySQL libmysqlclient Library mysql_real_connect() Buffer Overrun Vulnerability**
  A vulnerability has been reported for MySQL libmysqlclient library. The problem is said to occur in the mysql_real_connect() function and is likely due to insufficient bounds checking of user-supplied parameters.
  An attacker could potentially be capable of exploiting this issue to execute arbitrary code on a remote system. It should be noted that this issue would be required to be used in conjunction with an unrelated SQL injection attack or possibly used on a system which allows for the uploading of scripts.

- **Microsoft Messenger Service Buffer Overrun Vulnerability**
  Microsoft Messenger Service is prone to a remotely exploitable buffer overrun vulnerability. This is due to insufficient bounds checking of messages before they are passed to an internal buffer. Exploitation could result in a denial of service or in execution of malicious code in Local System context, potentially allowing for full system compromise.

Security Update 10

Symantec NetRecon 3.6 Security Update 10 (SU 10) detects and reports two vulnerabilities not resolved by Microsoft Internet Explorer Cumulative Patch Q822925 and enhances detection of three other vulnerabilities addressed by the patch. (See NetRecon SU9 "Internet Explorer" on page 148.)

Updated vulnerability detection

Security Update 10 detects and reports two vulnerabilities not addressed by patch Q822925.

- Microsoft Internet Explorer Browser Popup Window Object Type Validation Vulnerability
- Microsoft Internet Explorer XML Page Object Type Validation Vulnerability

This update also enhances detection of three vulnerabilities addressed by the patch.

- Microsoft Internet Explorer BR549.DLL ActiveX Control Buffer Overflow Vulnerability
- Microsoft Internet Explorer Object Type Validation Vulnerability
- Microsoft Internet Explorer Zone Restriction Bypass Script Execution Vulnerability

Microsoft patch Q828750 now supercedes patch Q822925.

Security Update 9

Symantec NetRecon 3.6 Security Update 9 (SU9) adds:

- Multithreading for PortCom, NRName, and NRWSockN modules.
- Detection and reporting of one new OpenSSH and five new Internet Explorer vulnerabilities.

Product enhancement

You can now optimize scans for PortCom, NRName, and NRWSockN modules by editing the modules.inf file and specifying the number of threads in the -t option. The default thread values are preferred.

These modules affect the following objectives:

- Discover SMTP vulnerabilities
- Discover FTP vulnerabilities

- Discover IRC vulnerabilities
- Discover HTTP vulnerabilities
- Discover HTTPS vulnerabilities
- Discover finger vulnerabilities
- Discover Oracle Database vulnerabilities
- Discover Trojans and vulnerable services running on TCP ports
- Discover vulnerable DCOM RPC services
- Identify network resources
- Enumerate target network resources
- Obtain banners from TCP services
- Similar objectives in the Granual Objectives section

New vulnerability detection

OpenSSH

- **OpenSSH Buffer Mismanagement Vulnerability**
  A buffer mismanagement vulnerability has been reported in OpenSSH. This issue exists in the buffer.c source file. A buffer structure size value may be expanded before the program attempts to reallocate the buffer using this size. If the expanded buffer size triggers a call to fatal(), a series of cleanup functions registered by the daemon will be called prior to exiting the program. One of these functions can reference buffer data—including the unused expanded value—causing a miscalculation. Depending on how cleanup functions reference this data, heap-based memory can be corrupted. The condition can reportedly be triggered by an overly large packet.

Internet Explorer

- **Microsoft Internet Explorer Browser Popup Window Object Type Validation**
  Internet Explorer does not properly handle object types when rendering malicious popup windows, allowing execution of malicious software. The problem occurs when Internet Explorer receives a response from a server after a malicious popup window containing an object tag has been parsed. Parameter checks of the type of file being loaded are not properly performed on the object type in HTTP responses received from the Web server.

- **Microsoft Internet Explorer XML Page Object Type Validation Vulnerability**
  Internet Explorer does not properly handle object types when rendering XML-based Web sites, allowing execution of malicious software. The problem occurs when Internet Explorer receives a response from a server after a malicious XML Web page containing an embedded object tag has been parsed. Exploitation of this vulnerability can cause malicious objects to be trusted, installed, and executed on the computer.

- **Microsoft Internet Explorer Object Type Validation Vulnerability**
  Internet Explorer does not properly handle object types when validating. Intruders can execute malicious software when Internet Explorer receives a response from a server after a Web page containing an object tag has been parsed. Exploitation of this vulnerability can cause malicious objects to be trusted and executed on the computer within the user's security context.

- **Microsoft Internet Explorer BR549.DLL ActiveX Control Buffer Overflow Vulnerability**
  Microsoft Internet Explorer BR549.dll ActiveX control is prone to a buffer overflow vulnerability. The issue is evident in the Windows reporting tool support functionality of BR549.dll, and is likely caused by insufficient bounds checking on user-supplied data. An attacker can leverage this issue to execute arbitrary instructions in the context of a user running an effected version of Microsoft Internet Explorer.

- **Microsoft Internet Explorer Zone Restriction Bypass Script Execution Vulnerability**
  A vulnerability in Internet Explorer can be exploited to execute arbitrary code within an otherwise inaccessible zone. Internet Explorer does not properly handle cached browser data, making it possible for a malicious Web script to access data within the My Computer zone. Exploitation of the vulnerability can give an attacker access to file contents or the ability to execute a file already present in the local file system of the My Computer zone. A malicious executable can also be placed in the user's Temporary Internet Files folder for later execution, possibly with the user's privileges. The vulnerability effects Internet Explorer 5.01, 5.5, and 6.0.

Security Update 8

Symantec NetRecon 3.6 Security Update 8 (SU8) adds detection and reporting of three additional vulnerabilities.

New vulnerability detection

- **Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability**
  The Microsoft RPCSS service is vulnerable to denial of service attacks. Other services dependant on RPCSS can also be effected. A vulnerability in the Windows DCE-RPC stack can be exploited to let a remote user disable RPC services. When an intentionally malformed packet is sent to the DCOM __RemoteGetClassObject interface, a NULL pointer is passed from __RemoteGetClassObject to the PerformScmStage function and the RPC service can fail. The vulnerability effects computers that have applied the patch for Microsoft Security Bulletin MS03-026.
- **Microsoft RPCSS DCOM Interface Long Filename Heap Corruption Vulnerability**
  A remotely exploitable heap corruption vulnerability has been discovered in RPC. The problem occurs in the RPCSS Service due to insufficient checks when handling length values in RPC DCOM filename parameters. By sending an exceptionally long string as the filename parameter, an intruder can corrupt sensitive locations in heap memory with user-supplied data. This lets a controlled word be written to an arbitrary location in memory, possibly allowing the execution of arbitrary code with SYSTEM privileges.
- **Microsoft RPCSS DCERPC DCOM Object Activation Packet Length Heap Corruption**
  A remotely exploitable heap corruption vulnerability has been discovered in RPC. The problem occurs in the RPCSS Service due to insufficient sanity checks when handling length values in DCERPC DCOM object activation packets. By transmitting a sequence of four or five of these malformed activation packets, an intruder can corrupt sensitive locations in heap memory with user-supplied data. As a result, an attacker may be capable of triggering a condition under which a controlled word may be written to an arbitrary location in memory. This could ultimately allow for the execution of arbitrary code with SYSTEM privileges.

Security Update 7

Symantec NetRecon 3.6 Security Update 7 (SU7) adds:

- Enhanced detection and reporting of the Microsoft DCOM RPC vulnerability.
- Detection and reporting of five new Apache vulnerabilities.
- One new scan objective.

New objectives

- **Discover vulnerable DCOM RPC services**
  This objective communicates directly with the RPC service and analyzes the response to detect systems that are vulnerable to exploits such as the Blaster worm and its variants.

New vulnerability detection

Microsoft Windows

- **DCOM RPC service vulnerable to the Blaster worm found**
  Microsoft Windows is prone to a buffer overrun vulnerability through the DCOM RPC interface. This can allow execution of arbitrary code. Remote attackers may execute malicious code, potentially resulting in full system compromise. Worms exploiting this vulnerability are currently in the wild. The vulnerable DCOM RPC service is detected by creating a RPC connection to the target and analyzing the response.

Apache Web Server

- **Apache HTTP Server Multiple Vulnerabilities**
  Apache HTTP Server version 1.3.28 has been released in response to multiple discovered vulnerabilities. Apache is vulnerable to three potential security issues. The impact of these vulnerabilities includes denial of service, file descriptor leakage, and logging failures.
- **Apache Web Server Type-Map Recursive Loop Denial Of Service Vulnerability**
  Apache content negotiation functionality is reportedly prone to a denial of service vulnerability. Under certain circumstances a local attacker may cause an Apache server to fall into an infinite loop, consuming resources exponentially and effectively denying service to legitimate system users.

- **Apache Web Server FTP Proxy IPV6 Denial Of Service Vulnerability**
  A denial of service vulnerability has been reported by the vendor to effect the Apache FTP proxy component. Reportedly an attacker may specify a target server that has an IPV6 address format. This may result in a denial of service to legitimate users.
- **Apache Web Server Prefork MPM Denial Of Service Vulnerability**
  The Apache Software Foundation has reported a vulnerability in the prefork MPM (Multi-Processing Module) that could result in a temporary denial of service.
- **Apache Web Server SSLCipherSuite Weak CipherSuite Renegotiation Weakness**
  The Apache Software Foundation has reported an issue that may occur when the SSLCipherSuite directive is used to upgrade a cipher suite. Particular sequences of per-directory renegotiations may cause this condition to occur, resulting in a weaker cipher suite being used in place of the upgraded one.

Security Update 6

Symantec NetRecon 3.6 Security Update 6 (SU6) detects any Windows 2000 and Windows XP systems susceptible to the “Blaster” worm.

Symantec NetRecon 3.6 Security Update 6 (SU6) adds detection and reporting of three states for Symantec Enterprise Security Architecture (SESA) and 78 vulnerabilities for Windows 2000 and Windows XP (1), Apache Web server (29), Hypertext Preprocessor (PHP) (16), Tomcat (18), and SSL (13).

New objectives

With the addition of SU6, Symantec NetRecon has four new objectives:

- Discover HTTPS vulnerabilities
- Discover network resources running SESA Manager
- Discover network resources running SESA Agents
- Discover network resources not running SESA Agents

Known issues

Microsoft Internet Explorer 6.0 or newer is required for the following objectives to run properly:

- Discover HTTP Vulnerabilities

- Discover network resources running SESA Manager

New state detection

With the addition of SU6, Symantec NetRecon can now detect and report the following states:

- **SESA Agent not detected**
  A system that may be able to run a SESA Agent was detected.
- **SESA Agent identified**
  A SESA Agent was detected.
- **SESA Manager detected**
  A SESA Manager is running.

New vulnerability detection

Microsoft Windows 2000 and Windows XP

- **Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability**
  Microsoft Windows is prone to a buffer overrun vulnerability via the DCOM RPC interface that could allow execution of arbitrary code. Remote attackers may execute malicious code on a vulnerable system, resulting in full system compromise. A worm exploiting this vulnerability is currently in the wild. Initial analysis suggests that the worm's executable file is named msblast.exe. SU6 detects UDP/TCP open ports 135, 139, and 445.

Apache Web Server

- **Apache APR_PSPrintf Memory Corruption Vulnerability**
  The Apache Software Foundation has released version 2.0.46, which addresses a vulnerability in the Web server. This is due to a potential memory management issue in the apr_psprintf() Apache Portable Runtime (APR) library. Exploitation could occur through mod_dav or other components. It is possible that exploitation could allow for execution of arbitrary code. Further details regarding this issue are pending from the vendor.
- **Apache Basic Authentication Module Valid User Login Denial Of Service**
  It has been reported that Apache 2.0 does not properly use specific thread-safe functions. Because of this, an attacker may be able to create a circumstance that prevents users from logging into restricted areas with valid user credentials.

- **Apache AB.C Web Benchmarking Buffer Overflow Vulnerability**
  A buffer overflow condition has been reported in the ab.c web benchmarking support utility that is provided with Apache Web server. It may be possible for a malicious attacker to exploit this overflow condition. The vulnerability is the result of improper bounds checking when processing command line options to ab. Since the program is not setuid, this vulnerability does not have a local impact. However, this may be an issue if the program is called from a CGI script. An attacker may be able to supply malformed command line parameters to the program, which will cause the overflow to occur. This vulnerability was originally discussed in BugTraq ID 5887. It is now being assigned an individual Bugtraq ID.

- **Apache AB.C Web Benchmarking Read_Connection() Buffer Overflow Vulnerability**
  A buffer overflow condition has been reported in the ab.c web benchmarking support utility that is provided with Apache Web server. It may be possible for a malicious Web server to exploit this overflow condition when the benchmarking utility is run against it. Data sent by a malicious server during the benchmarking process could cause memory to be corrupted with attacker-supplied values.

- **Apache Web Server Scoreboard Memory Segment Overwriting SIGUSR1 Sending**
  Apache is a freely available Web server for Unix and Linux variants, as well as Microsoft operating systems. A vulnerability in the handling of the Apache scorecard has been reported. A user with the privileges of the Apache user could attach to an httpd process and overwrite the parent[].pid and parent[].last_rtime shared memory segments. By overwriting these, a signal may be sent to an arbitrary process with administrative privileges.

- **Apache Server Side Includes Cross-Site Scripting Vulnerability**
  Apache is reported to be vulnerable to cross-site scripting attacks. This vulnerability is due to the SSI error pages of the Web server not being properly sanitized of malicious HTML code. Attacker-supplied HTML and script code may be executed on a Web client that is visiting the malicious link in the context of the Web server. Attacks of this nature may make it possible for attackers to manipulate Web content or to steal cookie-based authentication credentials. It may be possible to take arbitrary actions as the victim user.

- **Apache Web Server OS2 Filestat Denial Of Service Vulnerability**
  The Apache Software Foundation has reported a denial of service vulnerability on Apache for OS2 platforms. It is reported that device names can fault the OS2 worker process, which could result in a denial of service condition.

- **Apache Web Server File Descriptor Leakage Vulnerability**
  A vulnerability has been reported for Apache Web servers that may result in the disclosure of sensitive information. The vulnerability occurs due to the file descriptors being improperly inherited by child processes. Exploitation of this vulnerability may result in attackers being able to access sensitive log information.
- **Apache Web Server Linefeed Memory Allocation Denial Of Service Vulnerability**
  Apache Web servers are prone to a denial of service condition. This is due to how Apache handles excessive amounts of consecutive linefeed characters, which may cause the server to allocate large amounts of memory, resulting in a denial of service.
- **Apache 2 WebDAV CGI POST Request Information Disclosure Vulnerability**
  An information disclosure vulnerability has been reported for Apache. The vulnerability occurs due to inadequate checks being performed on CGI scripts. This vulnerability exists only when both WebDAV and CGI are enabled for folders. An attacker can exploit this vulnerability by making a POST request to a CGI script. Due to improper interaction between WebDAV and CGI scripts, this will result in the Web server returning the contents of the CGI script to the remote attacker.
- **Apache Web Server MIME Boundary Information Disclosure Vulnerability**
  A vulnerability has been discovered in the Apache Web server that may result in the disclosure of sensitive information. Specifically, sensitive process information is used within generated MIME message boundaries. Access to this information may aid an attacker in launching further attacks against target services. OpenBSD has released a patch that addresses this issue. MIME boundaries are now generated by the server using BASE64 encoded random numbers.
- **Apache Web Server ETag Header Information Disclosure Weakness**
  A weakness has been discovered in Apache Web servers that are configured to use the FileETag directive. Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields that are returned to a client contain the file's inode number. Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network. OpenBSD has released a patch that addresses this issue. Inode numbers that are returned from the server are now encoded using a private hash to avoid the release of sensitive information.

- **Apache Web Server Default Script Mapping Bypass Vulnerability**
  A vulnerability has been reported in the Apache Web browser that may result in the server bypassing existing default mappings when serving files. The vulnerability exists when making requests for files in directories with extensions. The vulnerability may cause the Web server to incorrectly parse the requested file. Instead of parsing the file "test" as a text file, the following request to www.target.com/folder.php/test results in Apache interpreting "test" as a PHP script.
- **Apache Web Server MS-DOS Device Name Denial Of Service Vulnerability**
  A vulnerability has been reported in Apache Web server for Microsoft Windows. The vulnerability exists in the way some HTTP requests are handled by the Apache Web server. Specifically, HTTP GET requests that involve reserved MS- DOS device names may cause the Apache Web server to crash.
- **Apache Web Server MS-DOS Device Name Arbitrary Code Execution Vulnerability**
  A vulnerability has been reported in Apache Web server for Microsoft Windows. The vulnerability exists in the way some HTTP requests are handled by the Apache Web server. Specifically, HTTP requests that involve MS-DOS device names may cause the Apache Web server to execute malicious attacker-supplied code. This exists if a malicious POST request is made to a CGI residing in a directory that is enabled with ScriptAlias.
- **Apache Web Server Illegal Character HTTP Request File Disclosure Vulnerability**
  A vulnerability has been reported in Apache Web server for Microsoft Windows 9x/Me operating environments. The vulnerability exists in the way some HTTP requests are handled by the Apache server. Any HTTP requests that end in some illegal characters will cause the server to disclose the contents of certain files to a remote attacker.
- **Apache HTPasswd Insecure Temporary File Vulnerability**
  Apache creates temporary files insecurely for htpasswd. As a result, it is possible for local attackers to read or corrupt the Apache password file. If the attacker can write custom-data to the password file, it may be possible to gain unauthorized access to resources that are protected by htpasswd. Alternatively, an attacker could reportedly read the password file and gain unauthorized access to credentials.
- **Apache /tmp File Race Vulnerability**
  Apache Web server is a popular http daemon, distributed with many variants of the UNIX Operating System and maintained by the Apache Project. Immunix is a hardened Linux distribution maintained by the Immunix team at the WireX Corporation. A problem has been discovered in

the Apache httpd that is distributed with the Immunix Linux distribution, a distribution based off the RedHat Linux distribution. Apache programs htdigest and htpasswd are used to offer advanced features to users of the Web server. However, these two helper programs insecurely create files in the /tmp directory, which could allow for /tmp file guessing. This makes it possible for a user with malicious motives to symlink attack files that are writable by the UID of the Apache process.

- **Multiple Apache HTDigest Buffer Overflow Vulnerabilities**
  Buffer overflow vulnerabilities have been reported to exist in the htdigest utility that is included with Apache. The vulnerability is due to improper bounds checking when copying user-supplied data into local buffers. This may be an issue if htdigest is called from a CGI script. An attacker may be able to supply malformed data to the program, which will cause the overflow to occur.

- **Apache HTDigest Arbitrary Command Execution Vulnerability**
  A vulnerability has been reported for Apache. Reportedly, the htdigest utility may be prone to a command execution vulnerability. The vulnerability is due to insecure system() calls when processing command line options. This may reportedly be an issue in circumstances where htdigest is called from a CGI script.

- **Multiple Apache HTDigest and HTPassWD Component Vulnerabilities**
  Apache is a freely available, open source Web server software package. It is distributed and maintained by the Apache Group. Multiple problems with Apache may lead to potential security vulnerabilities. The problems are in the htdigest.c and htpasswd.c files.

- **Apache 2 mod_dav Denial Of Service Vulnerability**
  A vulnerability has been discovered in the mod_dav component of Apache Web server. It has been reported that, under certain Apache configurations, it may be possible for an attacker to issue a malicious HTTP request that can result in a denial of service.

- **Apache Oversized STDERR Buffer Denial Of Service Vulnerability**
  Apache is prone to a denial of service condition when an excessive amount of data is written to stderr. This condition reportedly occurs when the amount of data that is written to stderr is more than the default amount that is allowed by the operating system. This may potentially be an issue in Web applications that write user-supplied data to stderr. Additionally, locally based attackers may exploit this issue. This issue has been confirmed in Apache 2.0.39/2.0.40 on Linux operating systems. Apache on other platforms may also be affected. This issue does not appear to be present in versions prior to 2.0.x.

- **Apache 2.0 CGI Path Disclosure Vulnerability**
  A path disclosure vulnerability has been reported in Apache 2.0.x. Apache will disclose the absolute path to a script whenever the server fails to invoke the script. If an attacker can create circumstances where the server will fail to invoke the script, then path information can be ascertained. Additionally, this information may be disclosed to arbitrary Web users whenever this type of error occurs.
- **Apache 2.0 Path Disclosure Vulnerability**
  A path disclosure vulnerability has been reported in Apache 2.0.x. It is possible to reproduce this condition on vulnerable systems by making a request for certain types of files (such as error documents) that have been mapped by the server by type but fail to be served due to failure of MIME negotiation.
- **Apache 2.0 Encoded Backslash Directory Traversal Vulnerability**
  A directory traversal vulnerability exists in Apache versions 2.0.39 and earlier on non-UNIX platforms (potentially including Apache compiled with CYGWIN). Platforms that may be affected by this include Windows, OS2, and Netware. The issue is related to the failure to properly process the backslash "\" character, which may be used as a directory delimiter under these platforms. By using the URL encoded sequence "%2e%2e%5c", the webroot directory may be escaped. Exploitation may result in the disclosure of sensitive information. Additionally, arbitrary local programs may be executed with attacker-supplied parameters if directory traversal techniques are used to escape the cgi-bin directory.
- **Apache httpd 2.0 CGI Error Path Disclosure Vulnerability**
  A minor information disclosure vulnerability has been reported in Apache httpd versions 2.0 to 2.0.35. A bug in the implementation of the ap_log_rerror() procedure, used to log server errors, may result in disclosure of absolute path information to remote clients. An absolute path on the Web server may be considered sensitive information. According to Apache, the vulnerability can be triggered by faulty CGI scripts.

Hypertext Preprocessor (PHP)

- **PHP Transparent Session ID Cross-Site Scripting Vulnerability**
  A cross-site scripting vulnerability has been discovered in PHP. The problem occurs due to insufficient sanitization of the PHPSESSID URI parameter. An attacker may be capable of exploiting this vulnerability by constructing a malicious link containing script code that is embedded within this variable. Successful exploitation of this issue would allow an attacker to execute arbitrary script code in a victim's browser within the

context of the visited Web site. This may allow for the theft of sensitive information or other attacks.

- **PHP STR_Repeat Boundary Condition Error Vulnerability**
  It has been reported that a buffer overrun exists in the PHP program. Because of this, an attacker may be able to execute arbitrary code.
- **PHP array_pad() Integer Overflow Memory Corruption Vulnerability**
  A vulnerability has been reported in PHP. The problem occurs in the array_pad() function and may allow an attacker to corrupt memory. The affected function reportedly fails to ensure that proper boundary checks are performed on values that are supplied by a malicious user. This may result in an integer overflow when array_pad() is called with an overly long value for its second argument. Further details of this vulnerability are currently unknown. This BID will be updated as more information becomes available.
- **PHP PHPInfo Cross-Site Scripting Vulnerability**
  Scripts that include the PHP phpinfo() debugging function may be prone to cross-site scripting attacks. This could permit remote attackers to create a malicious link to a vulnerable PHP script that includes hostile client-side script code or HTML. If this link is visited, the attacker-supplied code may be rendered in the browser of the user who visits the malicious link.
- **PHP Post File Upload Buffer Overflow Vulnerabilities**
  PHP is a widely deployed scripting language, designed for Web-based development and CGI programming. PHP does not perform proper bounds checking on functions that are related to Form-based File Uploads in HTML (RFC1867). Specifically, this problem occurs in the functions that are used to decode MIME encoded files. As a result, it may be possible to overrun the buffer that is used for the vulnerable functions to cause arbitrary attacker-supplied instructions to be executed. PHP is invoked through Web servers remotely. It may be possible for remote attackers to execute this vulnerability to gain access to target systems. A vulnerable PHP interpreter module is available for Apache servers that is often enabled by default.
- **PHP SafeMode Arbitrary File Execution Vulnerability**
  PHP is the Personal HomePage development toolkit, distributed by PHP.net, and maintained by the PHP development team in public domain. A problem with the toolkit could allow elevated privileges and potentially unauthorized access to restricted resources. A local user may upload a malicious php script and execute it with a custom query string. This makes it possible for a local user to execute commands as the HTTP process UID and potentially gain access with the same privileges of the HTTP UID. It has been reported that the proposed fix does not entirely fix the problem, as it's possible to pass command line parameters to sendmail when safe_mode is

enabled. This may be done through the fifth argument permitted by safe_mode.

- **PHP MySQL Safe_Mode Filesystem Circumvention Vulnerability**
  PHP is a server side scripting language, which is designed to be embedded within HTML files. It is available for Windows, Linux, and many UNIX-based operating systems. It is commonly used for Web development and is very widely deployed. The safe_mode feature in PHP may be used to restrict access to certain areas of a file system by PHP scripts. However, a problem has been discovered that may allow an attacker to bypass these restrictions to gain unauthorized access to areas of the file system that were restricted when PHP safe_mode was enabled. In particular, the MySQL client library that ships with PHP does not properly honor safe_mode. As a result, it is possible to use a LOAD DATA statement to read files that exist in restricted areas of the file system (as determined by PHP safe_mode).

- **PHP openlog() Buffer Overflow Vulnerability**
  A buffer overflow has been reported in the PHP openlog() function. By passing an argument of excessive size to the function, it may be possible for an attacker to overwrite memory, resulting in a denial of service. Although it has not been confirmed, it may be possible for an attacker to execute arbitrary commands within the PHP interpreter.

- **PHP emalloc() Unspecified Integer Overflow Memory Corruption Vulnerability**
  A vulnerability has been reported in PHP version 4.3.1 and earlier. The problem occurs in the emalloc() function and may allow an attacker to corrupt memory. The affected function reportedly fails to ensure that proper boundary checks are performed on values that are supplied by a malicious user. This may result in an integer overflow when emalloc() attempts to allocate memory. Further details of this vulnerability are currently unknown. This BID will be updated as more information becomes available.

- **PHP socket_recvfrom() Signed Integer Memory Corruption Vulnerability**
  A vulnerability has been reported in PHP versions 4.3.1 and earlier. The problem occurs in the socket_recvfrom() and may allow an attacker to corrupt memory. Specifically, the affected function fails to carry out sanity checks on user-supplied argument values, making it prone to an integer overflow. This may make it possible for an attacker to trigger a denial of service. Although it has not been confirmed, it may also be possible to exploit this issue to execute arbitrary code. It should be noted that socket functionality is included in PHP only if compiled with the "--enable-sockets" option.

- **PHP socket_recv() Signed Integer Memory Corruption Vulnerability**
  A vulnerability has been reported in PHP versions 4.3.1 and earlier. The problem occurs in the socket_recv() and may allow an attacker to corrupt memory. Specifically, the affected function fails to carry out sanity checks on user-supplied argument values, making it prone to an integer overflow. This may make it possible for an attacker to trigger a denial of service. Although it has not been confirmed, it may also be possible to exploit this issue to execute arbitrary code. It should be noted that socket functionality is included in PHP only if compiled with the "--enable-sockets" option.

- **PHP socket_iovec_alloc() Integer Overflow Vulnerability**
  A vulnerability has been reported in PHP versions 4.3.1 and earlier. The problem occurs in the socket_iovec_alloc() and may allow an attacker to corrupt memory. Specifically, the affected function fails to carry out sanity checks on user-supplied argument values, making it prone to an integer overflow. This may make it possible for an attacker to trigger a denial of service. Although it has not been confirmed, it may also be possible to exploit this issue to execute arbitrary code. It should be noted that socket functionality is included in PHP only if compiled with the "--enable-sockets" option.

- **PHP Mail Function ASCII Control Character Header Spoofing Vulnerability**
  PHP is the Personal HomePage development toolkit, distributed by PHP.net, and maintained by the PHP development team in public domain. The PHP mail function does not properly sanitize user input. Because of this, a user may pass ASCII control characters to the mail() function that could alter the headers of email. This could result in spoofed mail headers.

- **PHP wordwrap() Heap Corruption Vulnerability**
  A vulnerability has been discovered in PHP. A buffer overflow has been found in the wordwrap() function that may cause heap corruption when triggered. Memory corrupted by this issue may be later referenced by the calling Web server. It may be possible for a remote attacker to exploit this issue to overwrite an arbitrary word in memory. By redirecting program flow to point to malicious instructions, it may be possible for an attacker to execute arbitrary commands with the privileges of the vulnerable Web server.

- **PHP CGI SAPI Code Execution Vulnerability**
  The PHP CGI SAPI contains an unspecified bug that renders options for preventing direct access to the CGI binary useless. The configuration option "-- enable-force-cgi-redirect" and the php.ini option "cgi.force_redirect" could be disabled by this bug, allowing an attacker to gain access to any file that is readable by the Web server user. Arbitrary PHP code could also be executed.

- **PHP 4.0.3 IMAP Module Buffer Overflow Vulnerability**
  A vulnerability has been discovered in PHP 4.0.3. The problem occurs in the imap module when calling the imap_open() function. Exploitation of this issue may result in the target application crashing. Although it has not been confirmed, it may be possible to exploit this vulnerability to execute arbitrary code in the context of an application that uses the vulnerable function.

Tomcat

- **Apache Tomcat Insecure Directory Permissions Vulnerability**
  Apache Tomcat may be installed with insecure permissions for the /opt/tomcat/ directory. Files in this directory may contain sensitive information, such as authentication credentials. This issue was reported for Apache Tomcat versions prior to 4.1.24 on Gentoo Linux. It is not known if other distributions are similarly affected.
- **Apache Tomcat Invoker Servlet File Disclosure Vulnerability**
  An information disclosure vulnerability has been reported to exist in Apache Tomcat. The vulnerability allows an attacker to cause Tomcat to return the unprocessed source of a JSP page or, in certain circumstances, a resource that would have otherwise been secured. The vulnerability exists when using the invoker servlet in conjunction with the default servlet. This issue is a variant of the vulnerability that is described in BID 5786.
- **Apache Tomcat Example Web Application Cross-Site Scripting Vulnerability**
  A vulnerability has been reported for Apache Tomcat. Reportedly, it is possible for an attacker to launch a cross-site scripting attack. The cross-site scripting vulnerabilities exist in some sample Web applications that are distributed with Apache Tomcat 3.3.1a and earlier. This may enable a remote attacker to steal cookie-based authentication credentials from legitimate users of a host running Tomcat. Other attacks are also possible.
- **Apache Tomcat Web.XML File Contents Disclosure Vulnerability**
  Apache Tomcat is prone to a file disclosure vulnerability when used with JDK 1.3.1 or earlier. Apache Tomcat may permit malicious Web applications to read the contents of some files. It is possible to create a malicious "web.xml" file that is capable of reading parts of files. Any files that have content that can be read as part of an XML document would be disclosed to an attacker. This could result in disclosure of sensitive information.
- **Apache Tomcat Null Byte Directory/File Disclosure Vulnerability**
  Apache Tomcat is prone to a directory/file disclosure vulnerability when used with JDK 1.3.1 or earlier. It has been reported that remote attackers may view directory contents (even with an "index.html" or other welcome

file). It is also possible for remote attackers to disclose the contents of files. This vulnerability is due to improper handling of null bytes (%00) and backslash ("\") characters in requests for Web resources.

- **Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability**
  Multiple software and integrated server packages that function as Web proxies may be used as open TCP proxies. This is through the usage of the HTTP CONNECT method by default. This method is detailed in RFC 2817, where it is used to build generic Transit Layer Security over HTTP. Upon receiving a CONNECT request, vulnerable products act as a TCP proxy, tunneling the conversation. This can be used to launch attacks against internal machines or to use an internal mail server as an open relay. In many cases, this behavior may be controlled through the server configuration. Often it is related to support for tunneling or SSL-related functionality. The issue may also introduce an additional threat. Trusted, internal hosts may be able to proxy unauthorized connections to arbitrary ports on external hosts, which may violate security policy.
- **Apache Tomcat DefaultServlet File Disclosure Vulnerability**
  The servlet "org.apache.catalina.servlets.DefaultServlet" is included with Apache Tomcat by default. It is possible to use this servlet to view contents of files within the webroot directory. This includes JSP source code, which may contain sensitive data such as database user names and passwords.
- **Apache Tomcat 3.2 Directory Disclosure Vulnerability**
  Apache Tomcat is reported to be prone to a vulnerability that may enable remote attackers to disclose the contents of directories. This issue is reported to affect Apache Tomcat 3.2.x on HP-UX 11.04 (VVOS) systems. It is not known whether other systems are also affected.
- **Apache Tomcat 4.1 JSP Request Cross-Site Scripting Vulnerability**
  Jakarta Tomcat is a Java Servlet and JSP server that is produced by the Apache Software Foundation. Tomcat is available for Microsoft Windows, Linux, and other UNIX-based operating systems. A cross-site scripting vulnerability has been reported in some versions of Tomcat. Reportedly, if aN HTTP request is made for a JSP, malicious script code that is embedded in the URI may be included in a page that is generated by Tomcat. This may be related to the issues that are discussed in BID 2982. This has not, however, been confirmed.
- **Apache Tomcat Servlet Mapping Cross-Site Scripting Vulnerability**
  A vulnerability has been reported for Apache Tomcat 4.0.3 on Microsoft Windows and Linux platforms. Reportedly, it is possible for an attacker to launch a cross-site scripting attack. When servlet mapping is enabled, it is possible to invoke various servlets and classes and cause Apache Tomcat to throw an exception. This will make cross-site scripting attacks possible.

- **Apache Tomcat Null Character Malformed Request Denial Of Service Vulnerability**
  A vulnerability has been reported for Apache Tomcat 4.0.3 on a Microsoft Windows platform. Reportedly, it is possible for a remote attacker to make requests consisting of a large number of null characters to Tomcat that will cause the Web service to stop responding. By making numerous malformed requests, the attacker is able to exhaust all available threads for Tomcat, leading to the denial of service condition.

- **Apache Tomcat Web Root Path Disclosure Vulnerability**
  A vulnerability has been reported for Apache Tomcat on a Microsoft Windows platform. Reportedly, it is possible for a remote attacker to make requests that will result in Apache Tomcat returning an error page containing information that includes the absolute path to the server's webroot directory. For example, submitting a request for LPT9 to Tomcat will result in the following error message: "java.io.FileNotFoundException: C:\Program Files\Apache Tomcat 4.0\webapps\ROOT\lpt9 (the system cannot find the file specified)."

- **Apache Tomcat Example Files Web Root Path Disclosure Vulnerability**
  Apache Tomcat is a freely available, open source Web server that is maintained by the Apache Foundation. When Apache Tomcat is installed with a default configuration, several example files are also installed. When some of these example files are requested without any input, they will return an error containing the absolute path to the server's webroot directory.

- **Apache Tomcat JSP Engine Denial of Service Vulnerability**
  A vulnerability has been reported in Apache Tomcat for Windows that results in a denial of service condition. The vulnerability occurs when Tomcat encounters a malicious JSP page. The following snippet of code is reported to crash the Tomcat JSP engine: new WPrinterJob().pageSetup(null,null);

- **Apache Tomcat Source.JSP Malformed Request Information Disclosure Vulnerability**
  Apache Tomcat is a freely available, open source Web server that is maintained by the Apache Foundation. Under some circumstances, Tomcat may yield sensitive information about the Web server configuration. When the source.jsp page is passed a malformed request, it may leak information. This information may include the webroot directory and possibly a directory listing.

- **Apache Tomcat RealPath.JSP Malformed Request Information Disclosure**
  Apache Tomcat is a freely available open source Web server maintained by the Apache Foundation. Under some circumstances, Tomcat may yield

sensitive information about the Web server configuration. The realPath.jsp page may leak information when it is accessed. The realPath.jsp page displays the web root directory of the Tomcat implementation.

- **Apache Tomcat Servlet Path Disclosure Vulnerability**
  Apache Tomcat is a servlet container for use with the Java Servlet and JavaServer Pages technologies. Tomcat may be run on most UNIX and Linux variants as well as Microsoft Windows operating systems. Apache Tomcat ships with a number of example classes (SnoopServlet and TroubleShooter) which may reveal the absolute path of the Tomcat installation when requested. Disclosure of this type of sensitive information may aid in further attacks against the host running the vulnerable software.
- **Apache Tomcat System Path Information Disclosure Vulnerability**
  An issue has been reported in Apache Tomcat 4.1, which could reveal system path information to remote users. Submitting malformed requests may reveal an error message containing the absolute path to the webroot. Requests that allegedly cause the condition: http://target/+/file.jsp http://target/>/file.jsp http://target/</ file.jsp http://target/%20/file.jsp

SSL

- **OpenSSL Bad Version Oracle Side Channel Attack Vulnerability**
  A problem with OpenSSL may leak sensitive information. A user could abuse the response of vulnerable servers to act as an oracle. By sending a large number of adaptive attacks, the possibility exists for a remote user to create a choice of ciphertext that is encrypted with the private key of the server.
- **OpenSSL Timing Attack RSA Private Key Information Disclosure Vulnerability**
  A side-channel attack in the OpenSSL implementation has been published in a recent paper that may ultimately result in an active adversary gaining the RSA private key of a target server. The attack involves analysis of the timing of certain operations during client-server session key negotiation. Through this attack, it may be possible for a malicious client to discover the RSA private key of a server using the vulnerable software.
- **OpenSSL CBC Error Information Leakage Weakness**
  A side-channel attack against implementations of SSL exists that, through analysis of the timing of certain operations, can reveal sensitive information to an active adversary. The information that is leaked by vulnerable implementations is reportedly sufficient for an adaptive attack that ultimately obtains plaintext of a target block of ciphertext. The information loss was reduced in OpenSSL versions 0.9.6i and 0.9.7a. It is not known if other implementations are vulnerable to this or similar

weaknesses. It should be noted that this attack is reportedly difficult to exploit and requires that the adversary be a man-in-the-middle.

- **Mod_SSL Wildcard DNS Cross-Site Scripting Vulnerability**
  A vulnerability has been discovered in the mod_ssl module for Apache. It should be noted that the existence of this vulnerability is limited to configurations with both the "UseCanonicalName" option turned off and wildcard DNS enabled. It has been reported that Apache v1.x, when using the mod_ssl module will return an unescaped server name in response to HTTP requests on SSL ports. If all of these circumstances are met, an attacker may be able to exploit this issue via a malicious link containing arbitrary HTML and script code as part of the host name. When the malicious link is clicked by an unsuspecting user, the attacker- supplied HTML and script code will be executed by their Web client. This will occur because the server will echo back the malicious host name supplied in the client's request, without sufficiently escaping HTML and script code. Attacks of this nature may make it possible for attackers to manipulate Web content or to steal cookie-based authentication credentials. It may be possible to take arbitrary actions as the victim user.

- **OpenSSL SSLv2 Malformed . Overflow Vulnerability**
  OpenSSL is an open source implementation of the SSL protocol. It is used by a number of other projects, including but not restricted to Apache, Sendmail, Bind, etc. It is commonly found on Linux and UNIX-based systems. A buffer overflow vulnerability has been reported in some versions of OpenSSL. A buffer overflow has been reported in the handling of the client key value during the negotiation of the SSLv2 protocol. A malicious client may be able to exploit this vulnerability to execute arbitrary code as the vulnerable server process or possibly to create a denial of service condition. UPDATE: A worm has been discovered propagating in the wild that likely exploits this vulnerability. Additionally, this code includes peer-to-peer and distributed denial of service capabilities. There are have been numerous reports of intrusions in Europe. It is not yet confirmed whether this vulnerability is in OpenSSL, mod_ssl, or another component. Administrators are advised to upgrade to the most recent versions or disable Apache, if possible, until more information is available.

- **OpenSSL SSLv3 Session ID Buffer Overflow Vulnerability**
  A vulnerability has been reported for OpenSSL. The vulnerability affects SSLv3 session IDs. Reportedly when a an oversized SSL version 3 session ID is supplied to a client from a malicious server, it is possible to overflow a buffer on the remote system. This could result in key memory areas on the vulnerable, remote system being overwritten and possibly lead to the execution of arbitrary code as the client process.

- **OpenSSL ASN.1 Parsing Error Denial Of Service Vulnerability**
  A remotely exploitable denial of service condition has been reported in the OpenSSL ASN.1 library. This vulnerability is due to parsing errors and affects SSL, TLS, S/MIME, PKCS#7 and certificate creation routines. In particular, malformed certificate encodings could cause a denial of service to server and client implementations that depend on OpenSSL.
- **OpenSSL Kerberos Enabled SSLv3 Master Key Exchange Buffer Overflow**
  A vulnerability has been reported for OpenSSL 0.9.7 pre-release versions. When initiating contact between a SSLv3 server, master keys are exchanged between the client and the server. When an oversized master key is supplied to a SSL version 3 server by a malicious client, it may cause a buffer to overflow on the vulnerable system. Execution of arbitrary code as the server process may be possible. This vulnerability is present only when Kerberos is enabled for a system using SSL version 3.
- **OpenSSL ASCII Representation Of Integers Buffer Overflow Vulnerability**
  Remotely exploitable buffer overflow conditions have been reported in OpenSSL. This issue is due to insufficient checking of bounds with regards to ASCII representations of integers on 64 bit platforms. It is possible to overflow these buffers on a vulnerable system if overly large values are submitted by a malicious attacker. Exploitation of this vulnerability may allow execution of arbitrary code with the privileges of the vulnerable application, service, or client.
- **Mod_SSL Off-By-One HTAccess Buffer Overflow Vulnerability**
  An off-by-one issue exists in mod_ssl that affects Apache when handling certain types of long entries in a .htaccess file. Though this capability within the Web server is not enabled by default, it is popular because it allows non-privileged users to create Web access control schemes for hosted sites and is enabled through the "AllowOverride" configuration variable in Apache. A .htaccess file with 10,000 or more bytes set into the variable DATE_LOCALE results in a buffer overflow within the Web server process handling the request.
- **Apache mod_ssl/Apache-SSL Buffer Overflow Vulnerability**
  Mod_SSL and Apache-SSL are implementations of SSL (Secure Socket Layer) for the Apache Web server. A buffer overflow vulnerability exists in mod_ssl and Apache-SSL that may allow for attackers to execute arbitrary code. The overflow exists when the modules attempt to cache SSL sessions. Vulnerable versions of mod_ssl and Apache-SSL are incapable of handling large session representations. To exploit this vulnerability, the attacker must somehow increase the size of the data representing the session. This may be accomplished through the use of an extremely large client certificate. This is possible only if verification of client certificates is enabled and if the certificate is verified by a CA trusted by the Web server.

Though these requirements make this vulnerability theoretical, administrators are still urged to upgrade.

- **OpenSSL PRNG Internal State Disclosure Vulnerability**
  The randomness pool and associated mixing function that are used by the OpenSSL PRNG (pseudo-random number generator) suffer from a flaw that could enable an attacker to reconstruct the generator's internal state. The flaw exists because the data quantum used for generator output is derived from a hash value to which the same portion of secret internal state data was input. In general, this means the state data can no longer be considered secret. The number of requested PRNG output bytes can be as low as one, allowing for brute-force analysis of all possible cases. If an attacker is able to gain knowledge of the generator's state, it may be possible for that attacker to predict future results. The impact of this vulnerability depends on the nature of the target application or protocol. It is relatively unlikely for data to be retrieved from the OpenSSL PRNG in a pattern allowing for attacks. No vulnerable applications are currently known.

- **OpenSSL Unseeded Random Number Generator Vulnerability**
  A design error exists in some versions of OpenSSL that may lead to the disclosure of sensitive information. The problem exists because the SSL_connect() function, which is used to initiate the TLS/SSL handshake with a server, does not ensure that the underlying pseudo-random number generator is properly seeded before initiating a SSL connection. This may lead to the disclosure of sensitive information by applications using the OpenSSL toolkit if the random number generator is not initialized. This problem is known to affect qmail's unofficial "tls.patch" patch, which fails to seed the random number generator.

Security Update 5

Symantec NetRecon 3.6 Security Update 5 (SU5) adds detection and reporting of four new wireless access point vulnerabilities

New vulnerability detection

With the addition of SU5, Symantec NetRecon can now detect and report the following vulnerabilities:

- **Corega Wireless Access Point Identified**
  A Corega wireless access point could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities.
- **IOData Wireless Access Point Identified**
  A IOData wireless access point could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities.
- **Melco Wireless Access Point Identified**
  A Melco wireless access point could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities.
- **Melco Wireless Access Point Identified via SNMP**
  A Melco wireless access point via SNMP could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities. SNMP is also considered an insecure protocol.

Security Update 4

Symantec NetRecon 3.6 Security Update 4 (SU4) adds detection and reporting of 51 additional vulnerabilities for Samba (14), sendmail (13), MySQL (18), Cisco (4), and Microsoft (2).

New vulnerability detection

With the addition of SU4, Symantec NetRecon can now detect and report the following vulnerabilities:

Samba

- **Samba call_trans2open Remote Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in Samba 2.2.8 and earlier and in Samba-TNG 0.3.1 and earlier could let an attacker execute arbitrary commands with the privileges of the Samba process. When copying user-supplied data into a static buffer, passing excessive data to an affected Samba server could let an anonymous user corrupt sensitive locations in memory.
- **Samba Multiple Unspecified Remote Buffer Overflow Vulnerabilities**
  Multiple remote buffer overflow vulnerabilities in Samba 2.2.8 and Samba-TNG 0.3.1 could let an attacker execute arbitrary code with the privileges of Samba, typically root.
- **Samba-TNG Unspecified Remote Privilege Escalation Vulnerability**
  A privilege escalation vulnerability in Samba-TNG could let an anonymous remote attacker gain root privileges.
- **Samba SMB/CIFS Packet Assembling Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in Samba could let an attacker create a specially formatted SMB/CIFS packet that could cause smbd to overwrite sensitive areas of memory with attacker-supplied values. This vulnerability is especially severe because the smbd service runs with root privileges.
- **Samba REG File Writing Race Condition Vulnerability**
  A race condition vulnerability in Samba could let an attacker corrupt local files with custom data and gain elevated privileges. An attacker could create a symbolic link at a crucial point of program execution that would overwrite Samba reg files. This can only occur if the files are writable by the Samba process.
- **Samba Server Encrypted Password Buffer Overrun Vulnerability**
  A buffer overflow vulnerability in the password change request routine used in Samba could let an attacker execute arbitrary code with superuser privileges. Insufficient bounds checking of user supplied input could let an attacker pass an encrypted password of excessive length to smbd. Applications implementing the pam_smbpass PAM module can be locally exploited. This condition could also be exploited remotely, potentially resulting in the execution of arbitrary code with superuser privileges.
- **Samba Improperly Terminated Struct Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in Samba version 2.2.4, due to improper termination of memory structures, could result in the execution of arbitrary code.

- **Samba Remote Arbitrary File Creation Vulnerability**
  A vulnerability in Samba could let a remote or local user overwrite files, gain elevated privileges, and deny service to legitimate users. The smbd service does not sufficiently check NetBIOS name input.
- **Samba Insecure TMP file Symbolic Link Vulnerability**
  A vulnerability in Samba could let an attacker cause a denial of service and gain elevated privileges. A user could create a symbolic link to files owned by privileged users in the system and write data to those files, such as system device files.
- **Samba SWAT Symlink Vulnerability**
  A vulnerability in Samba SWAT (Samba Web Administration Tool) could let local users gain root access. By default, SWAT logs to /tmp/cgi.log. An attacker could use symlink to overwrite files such as /etc/passwd with user specified data.
- **Samba SWAT Logging Failure Vulnerability**
  A vulnerability in Samba SWAT (Samba Web Administration Tool) could let remote users gain access to the network. Certain versions of SWAT do not log bad login attempts if the remote user enters a correct user name but wrong password. This lets remote users continuously guess passwords without being logged or locked out.
- **Samba SWAT Logfile Permissions Vulnerability**
  A vulnerability in Samba SWAT (Samba Web Administration Tool) could let local users gain root access. Poor permission settings in SWAT's log files (/tmp/cgi.log by default) could let attackers read user name and password data that SWAT records for remote users.
- **Samba Pre-2.0.5 Vulnerabilities**
  Several vulnerabilities in versions of Samba prior to 2.0.5 could let an attacker perpetrate a denial of service or buffer overflow attack.
  Nmbd (the NetBIOS name service or daemon) could be exploited for a denial of service. A function in the messaging system of smbd could let an attacker execute arbitrary code as root if the message command is set in smb.conf, creating a buffer overflow. And a race condition vulnerability could let an attacker mount arbitrary points in the file system if smbmnt is setuid root.
- **Samba Long Password Buffer Overflow Vulnerability**
  A vulnerability in the password function of the authentication mechanism in older versions of Samba could let an attacker supply an overly long password to the Samba server, triggering a buffer overflow.

Sendmail

- **Sendmail Address Prescan Memory Corruption Vulnerability**
  A logic vulnerability in the conversion of a character to an integer value during the prescan() procedure of sendmail versions prior to 8.12.9 could let a remote attacker execute arbitrary code.
- **Sendmail check_relay Access Bypassing Vulnerability**
  A vulnerability in sendmail could let attackers use bogus DNS data to bypass the access restrictions imposed by the access_db FEATURE when used with the check_relay ruleset, allowing unauthorized access.
- **Sendmail Trojan Horse Vulnerability**
  The sendmail ftp server (ftp.sendmail.org) was compromised. Sendmail source code that was downloaded from ftp.sendmail.org between September 28, 2002 and October 6, 2002 likely contains trojan horse code. Versions of sendmail downloaded via HTTP was not affected.
- **Sendmail SMRSH Double Pipe Access Validation Vulnerability**
  A vulnerability in smrsh (restricted shell for sendmail) could let an attacker execute commands outside of the restricted environment. When commands are entered using either double pipes (||) or a mixture of dot (.) and slash (/) characters, a user could bypass the checks performed by smrsh.
- **Sendmail Long Ident Logging Circumvention Weakness**
  A vulnerability in the way sendmail handles long indents could let an attacker attempt certain commands without the attacking IP address being logged.
- **Sendmail DNS Map TXT Record Buffer Overflow Vulnerability**
  A vulnerability in sendmail's DNS handling code could let a malicious nameserver send a string of arbitrary length, resulting in a buffer overflow and the execution of arbitrary code. When sendmail attempts to map an address using a TXT query type, it does not properly check bounds on data returned from the nameserver.
- **Sendmail File Locking Denial Of Service Vulnerability**
  A vulnerability in sendmail could let a user acquire an exclusive lock on files that sendmail requires for operation, resulting in a denial of service.
- **Sendmail Inadequate Privilege Lowering Vulnerability**
  A vulnerability in the config file parser of sendmail version 8.12.0 could let an attacker re-acquire higher privileges through the effective group. In this version, the sendmail utility is setgid instead of setuid. The code that drops privileges does not lower the saved groupid making it possible to reclaim the effective groupid if an attacker can force the process to call setregid().

- **Sendmail Queue Processing Data Loss/DoS Vulnerability**
  A vulnerability in sendmail could let attackers cause a loss of data or a denial of service. Sendmail users could change key configuration variables (such as setting the message hop count to a value greater than the limit imposed by sendmail) causing mail in the queue to be dropped.
- **Sendmail Debugger Arbitrary Code Execution Vulnerability**
  An input validation error in sendmail's debugging functionality could let an attacker gain full access to the network. Sendmail's tTflag() function processes arguments supplied from the command line with the -d switch and writes the values to its internal trace vector. Supplying a large numeric value for the category part of the debugger arguments could cause a signed integer overflow. The numeric value is used as an index for the trace vector. If a negative value is given, an attacker could write to a certain range of process memory. Because the -d switch is processed before the program drops its elevated privileges, this could lead to a full system compromise.
- **Sendmail Unsafe Signal Handling Race Condition Vulnerability**
  Several race condition vulnerabilities in sendmail, using non-atomic or non-reentrant operations in signal handling functions, could cause undesired or unexpected behavior.
- **Sendmail ETRN Denial of Service Vulnerability**
  A vulnerability in sendmail could let an attacker cause a low-bandwidth denial of service or a reboot of the server. When a client connects to the sendmail smtpd and sends an ETRN command to the server, the server fork()s and sleeps for 5 seconds. If many ETRN commands are sent to a server, it is possible to exhaust system resources.
- **Sendmail Aliases Database Regeneration Vulnerability**
  A vulnerability in sendmail could let a malicious user corrupt the aliases database. To regenerate the sendmail aliases database, sendmail is run locally with the -bi parameters. No checks are made against the user privileges to determine whether they are authorized. It is therefore possible to regenerate the aliases database and then interrupt it, corrupting the database.

MySQL

- **MySQL Weak Password Encryption Vulnerability**
  A weak password encryption algorithm in MySQL could let an attacker gain access to passwords and other encrypted information. The function used to encrypt MySQL passwords makes only one pass over the password and employs a weak left shift based cipher. The hash could be cracked easily using a brute force method.

- **MySQL mysqld Privilege Escalation Vulnerability**
  A vulnerability in MySQL could let an attacker use the mysqld service with elevated privileges. If DATADIR/my.cnf includes the line **user=root** under the **[mysqld]** option section, the mysqld service runs as root user rather than the default user.
- **MySQL Double Free Heap Corruption Vulnerability**
  A vulnerability in MySQL could let an attacker cause a denial of service. A malicious MySQL client could force MySQL to attempt to free the same memory twice.
- **MySQL COM_CHANGE_USER Password Memory Corruption Vulnerability**
  A memory corruption vulnerability in the COM_CHANGE_USER command of MySQL could let an attacker execute arbitrary code in the security context of the MySQL server process. A lack of sufficient bounds checking for client responses to password authentication challenges could let the attacker overwrite the saved instruction pointer on the stack with bytes generated by the random number generator of the password verification algorithm.
- **MySQL COM_CHANGE_USER Password Length Account Compromise Vulnerability**
  A vulnerability in the password authentication mechanism for MySQL could let an authenticated database user compromise the accounts of other database users. When the COM_CHANGE_USER command is issued to iterate through a comparison during authentication, MySQL uses a string returned by the client. Attackers could authenticate as another database user if they can successfully guess the first character of the correct password for that user. The range of the valid character set for passwords is 32 characters, which means that a malicious user can authenticate after a maximum of 32 attempts if they cycle through all of the valid characters.
- **MySQL libmysqlclient Library Read_Rows Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in the read_rows function of the MySQL libmysqlclient library could let an attacker cause a denial of service or possibly execute arbitrary code in the security context of the MySQL client. The MySQL client does not verify that the stored row sizes are smaller than the destination buffer. Anything that is linked against libmysql could also be affected by this vulnerability.
- **MySQL libmysqlclient Library Read_One_Row Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in the read_one_row function of the MySQL libmysqlclient library could let an attacker cause a denial of service. The

MySQL client does not verify that the stored row sizes are smaller than the destination buffer.

- **MySQL COM_TABLE_DUMP Memory Corruption Vulnerability**
  A memory corruption vulnerability in MySQL could let an attacker cause a denial of service by causing a malformed COM_TABLE_DUMP server command to be issued with malformed parameters.
- **MySQL DataDir Parameter Local Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in MySQL could let an attacker corrupt memory and possibly execute arbitrary commands within the context of the SYSTEM user.
- **MySQL Logging Not Enabled Weak Default Configuration Vulnerability**
  A weak default configuration in MySQL could let a user attack the database undetected by the administrator. By default, most logging is disabled in MySQL.
- **MySQL Null Root Password Weak Default Configuration Vulnerability**
  A weak default configuration in the Windows binary release of MySQL could let an attacker gain root access to the database. The root user of the database is defined with no password and is granted login privileges from any host.
- **MySQL Bind Address Not Enabled Weak Default Configuration Vulnerability**
  A weak default configuration in the Windows binary release of MySQL could let a remote attacker gain access to default installations of the server. By default, MySQL does not enable the bind-address configuration directive.
- **MySQL Root Operation Symbolic Link File Overwriting Vulnerability**
  A vulnerability in MySQL databases that are configured with a uid of root could let users with the CREATE TABLE privilege overwrite sensitive system files and possibly gain elevated privileges. By using a symbolic link in the /var/tmp directory and linking it to a file that is write-accessible by root, a user could log into the database with their account and create a table with a name corresponding to that of the symbolic link. The creation of the table overwrites the linked file and any data created within the table is written to the file that has been symbolically linked.
- **MySQL SHOW GRANTS Password Hash Disclosure Vulnerability**
  A vulnerability in MySQL could let an attacker using the SHOW grants query obtain encrypted passwords. Using a dictionary attack, an attacker could read these password hashes and further compromise user accounts.

- **MySQL Local Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in MySQL could let an attacker overwrite critical parts of the stack frame such as the calling function's return address. Supplying an excessively long string as an argument for a SELECT statement could let a local attacker overflow the MySQL query string buffer.
- **MySQL Unauthenticated Remote Access Vulnerability**
  A vulnerability in the password verification scheme in MySQL could let unauthorized users access the database. Once MySQL grants access to a machine, any user on that machine can connect to the database. Instead of having to know an account name and password, the attacker need only know a legitimate account name.
- **MySQL Authentication Algorithm Vulnerability**
  An authentication vulnerability in MySQL could let an attacker gain unauthorized access to the server. There are arithmetic properties in MySQL authentication check-strings that are consistent throughout multiple authentications. If multiple client authentications are observed by an attacker, the password hash can be deduced.
- **MySQL GRANT Global Password Changing Vulnerability**
  A vulnerability in MySQL could let users with GRANT access change passwords in the database (including the superuser password). In addition, MySQL ships with a test account with GRANT privileges and that is not protected with a password. These two problems combined can result in a total, remote (and probably anonymous) database compromise. The database can be compromised even if the test account is disabled (given a local user account with GRANT privileges).

Cisco

- **Cisco Catalyst CatOS Authentication Bypass Vulnerability**
  A vulnerability in Cisco Catalyst switches could let an attacker with command line access gain unauthorized access to the enable mode without a password.
- **Cisco Catalyst Unicast Traffic Broadcast Vulnerability**
  A vulnerability in Cisco Catalyst could let an attacker cause a denial of service. Cisco Catalyst does not always capture the MAC address until after several packets are sent to the unknown host. Unicast traffic could be broadcast to all systems connected to the switch.
- **Cisco Catalyst ssh Protocol Mismatch Denial of Service Vulnerability**
  A vulnerability in versions 6.1(1), 6.1(1a) and 6.1(1b) of Catalyst 4000, 5000, and 6000 devices with SSH enabled and supporting 3 DES encryption could let an attacker cause a denial of service. If a connection is made to the SSH

service on a vulnerable Catalyst device and the protocol mismatch error occurs, the device will reset. The supervisor engine will fail and be unable to handle the error.

- **Cisco Catalyst Enable Password Bypass Vulnerability**
  A vulnerability in Cisco Catalyst could let a user gain unauthorized access. Users who already have access to the device can elevate their current access to enable mode without a password. Once enable mode is obtained users can access the configuration mode and commit unauthorized configuration changes from the console itself or via a remote Telnet session.

Microsoft

- **Microsoft Windows RPC Service Denial of Service Vulnerability**
  A vulnerability in the RPC service of Microsoft Windows 2000, Windows NT 4.0, and Windows XP could let a remote attacker cause a denial of service. Sending a specifically malformed packet to TCP port 135 could disable the RPC service.
- **Microsoft IIS WebDAV Denial Of Service Vulnerability**
  A vulnerability in Microsoft IIS 5 and 5.1 could let an attacker cause a denial of service. Specially crafted WebDAV requests could result in IIS allocating an extremely large amount of memory on the server.

Security Update 3

Symantec NetRecon 3.6 Security Update 3 (SU3) adds detection and reporting of seven Microsoft Internet Explorer vulnerabilities, twenty-one Cisco vulnerabilities, eleven IBM Lotus Domino vulnerabilities, ten wireless network vulnerabilities, and vulnerabilities that relate to Microsoft Exchange Server and VPN.

New vulnerability detection

With the addition of SU3, Symantec NetRecon can now detect and report the following vulnerabilities:

- **IE is vulnerable to arbitrary code injection through malformed header fields**
  A vulnerability in Internet Explorer 5.01 and 6.0 could let remote attackers execute arbitrary code using malformed content-disposition and content-type header fields. This could let the application for the spoofed file type pass the file back to the operating system for handling instead of producing an error message.

- **System Attendant on Exchange Server 2000 grants unauthorized registry access**
  System Attendant on Microsoft Exchange Server 2000 grants Everyone privileges to the WinReg key, letting remote attackers read or modify registry keys.

- **Microsoft IE Arbitrary File Execution Vulnerability**
  Microsoft Internet Explorer mishandles conflicting information in some HTTP headers that are used to describe non-HTML content. A malicious Web server could provide content with misleading values in the content-type and content-disposition header fields. Under these circumstances, IE could automatically download and execute arbitrary programs. This vulnerability can also be exploited through HTML formatted email.

- **Microsoft IE HTTP Request Encoding Vulnerability**
  A vulnerability in Microsoft Internet Explorer could let an attacker craft a URL that redirects a user to a third-party Web site. This redirection could also include commands that would appear to have come from the user.

- **Microsoft IE Zone Spoofing Vulnerability**
  A vulnerability in Microsoft Internet Explorer in the way it handles Web sites that are accessed using the NetBIOS protocol could allow malicious Web sites to be viewed in the Local Intranet Zone. A maliciously crafted Web page could trick IE into opening the page as a trusted site.

- **Microsoft IE Arbitrary Program Execution Vulnerability**
  A vulnerability in Microsoft Internet Explorer could let malicious Web sites execute programs on client systems. If an object is embedded in HTML with a non-zero CLASSID value and the CODEBASE parameter is set to the path of an executable on the client system, the specified program will execute. Later versions of IE included a fix for this vulnerability, but IE may still be vulnerable. If objects with a CODEBASE value that is set to execute on the client system are embedded in new objects using window.PoPup() or window.Open(), the specified program will execute.
  Also, it may be possible for an attacker to execute programs on target systems originating from remote machines. Programs on shares could be downloaded and executed on client systems automatically. For example, an attacker could conceivably place a trojan program on a host with a world-accessible share. If the address of the share and the path of this program are set as the CODEBASE value, the program may execute.

- **Microsoft IE Same Origin Policy Violation Vulnerability**
  A vulnerability in Microsoft Internet Explorer could let users circumvent the “same origin policy.” In modern browsers, script code executing in the context of one Web site should not be able to access the properties of another. This security feature is known as the “same origin policy,” and it

aims to prevent malicious Web sites from interacting with and possibly stealing sensitive information from other sites in different windows. When one Web site (“parent”) opens another Web site in a new window (“child”) using the document.Open() method, script code in the parent Web site could interact with properties of the child Web site.

- **Microsoft IE Forced Script Execution Vulnerability**
  A vulnerability in Microsoft Internet Explorer could allow script code to be executed despite properly configured security settings. IE does not check all event handlers. Script code could execute if it is embedded in Web content as handlers for asynchronous events. Setting “Active Scripting” to “Disable” will not prevent the execution of the script.
- **VPN service enabled**
  A Virtual Private Network (VPN) server usually implements Point to Point Tunneling Protocol (PPTP), allowing remote users to access the internal network.
- **Cisco IOS TFTP Server Long File Name Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in older versions of Cisco IOS (before version 12.0) could result in denial of service and malicious code execution. Due to insufficient bounds checking on requested file names, a request for a file name of 700 or more bytes could cause the router to crash and reboot.
- **Cisco IOS ILMI SNMP Community String Vulnerability**
  A vulnerability in Cisco IOS versions 11.x and 12.0 could let an unauthorized user access certain Cisco configuration variables. The ILMI SNMP community string allows read and write access to system objects in the MIB-II community group. A malicious remote user could change configuration objects within the MIB-II community, rename the system, change the location name in the system, and change the contact information for the system.
- **Cisco IOS Malformed PPTP Packet Denial of Service Vulnerability**
  A vulnerability in Cisco IOS versions that support the Point to Point Tunneling Protocol (PPTP) could let remote users disable a Cisco router. If a malformed PPTP packet is sent to port 1723 on a vulnerable router, the router must be reset to regain normal functionality.
- **Multiple Vendor Session Initiation Protocol Vulnerabilities**
  Vulnerabilities related to handling of SIP INVITE messages in Session Initiation Protocol (SIP) implementations could be exploited to cause a denial of service and may allow unauthorized access.

- **Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in versions 5.4 through 7.4 of Cisco CatOS HTTP Server could be exploited for a denial of service if the Cisco image name contains “cv.”

- **Cisco Switch Router with Fast Ethernet Cards ACL Bypass/DoS Vulnerabilities**
  A vulnerability in Cisco Gigabit Switch Routers (GSRs), when used with configured Fast Ethernet/Gigabit Ethernet cards, could let attackers bypass access control lists (ACLs). An attacker could prevent the interface on the target GSR from stopping the forwarding of packets, resulting in a denial of service. All versions of IOS greater than 11.2 on GSRs are assumed to be vulnerable.

- **Cisco IOS Router Scan Software Reloading Vulnerability**
  A vulnerability in Cisco IOS could result in an arbitrary reload of the router configuration, and potentially a denial of service. A TCP scan against Cisco routers (3100-3999, 5100-5999, 7100-7999, and 10100-10999) can cause the router to become unstable and suffer memory corruption. A subsequent attempt to access the configuration could cause the router to reload the configuration.

- **Cisco Catalyst 802.1x Frame Forwarding Vulnerability**
  A vulnerability in the 5000 and 2900 series Cisco Catalyst Switch could be exploited for a denial of service. Sending an 802.1x frame to a switch with spanning tree protocol blocked port could result in a storm of 802.1x frames being forwarded to the VLAN that is managed by the switch.

- **Cisco Catalyst Memory Leak Denial of Service Vulnerability**
  A vulnerability in the telnet server that is shipped with Catalyst firmware could be exploited for a denial of service. Each time that the telnet service is started, memory resources are used without being freed. Connecting multiple clients to the Catalyst telnet server depletes memory, leaving the device unable to function properly and vulnerable to a denial of service until the device is manually reset.

- **Cisco SSH Denial of Service Vulnerability**
  While addressing previous vulnerabilities, a denial of service condition was inadvertently introduced into firmware upgrades for Cisco routers and switches (IOS). Catalyst 6000 switches running CatOS, Cisco PIX Firewall, and Cisco 11000 Content Service Switch devices may be vulnerable. Scanning for SSH vulnerabilities on affected devices can cause excessive CPU consumption due to a failure of the Cisco SSH implementation to properly process large SSH packets. Repeated and concurrent attacks can result in a denial of service.

- **Cisco Local Interface ARP Denial of Service Vulnerability**
  A vulnerability in Cisco IOS could facilitate a denial of service by a user on a system that is local to the router. When multiple ARP requests are sent to the router, it makes an entry for its own MAC address as the received address. Afterwards, the router discontinues all other ARP entries.
- **Cisco IOS Cisco Express Forwarding Session Information Leakage Vulnerability**
  If Cisco Express Forwarding is enabled, a vulnerability in Cisco IOS could expose packet information to unintended recipients. If a packet that is sent to a router has a MAC layer packet length that is shorter than that specified in the IP layer length, the packet is padded by the router before being routed. The data that are used to pad the packet are taken from previously routed packets that are still in the router's memory.
- **Cisco 12000 Series Internet Router Denial Of Service Vulnerability**
  A vulnerability in Cisco 12000 Series Internet Routers could result in a denial of service. Sending large numbers of ICMP unreachable packets could overburden CPU resources and prevent the forwarding of packets. This condition may occur when the router is "Black Hole" filtering.
- **Cisco Access Control List Fragment Non-blocking Vulnerability**
  A vulnerability in IOS on Cisco 12000 series routers with Engine 2 based cards could let users communicate with protected hosts, bypassing the security policy. Affected routers do not properly filter fragmented packets with access control entries. Non-initial fragmented packets that are sent to a protected host can bypass the ACL.
- **Cisco 12000 Series Internet Router ACL Failure To Drop Packets Vulnerability**
  A vulnerability in Cisco 12000 Series Internet Routers with line cards that are based on Engine 2 could let restricted traffic into the network. When an outgoing access control list (ACL) is exactly 448 lines and the last statement is not explicitly a "deny ip any any" rule, some packets are not properly dropped.
- **Cisco Outbound Access Control List Bypass Vulnerability**
  A vulnerability in IOS on Cisco 12000 series routers with Engine 2 based cards could fail to block traffic using outbound ACLs. Routers are vulnerable when the input ACL is configured on some, but not all, of the interfaces on the card. Routers are vulnerable only when the packets in question are not blocked by an inbound ACL on the ingress port. An ACL that is applied to incoming packets will still behave as expected.
- **Cisco 12000 Outgoing ACL Fragmented Packet Vulnerability**
  A vulnerability in IOS on Cisco 12000 series routers with Engine 2 based cards could fail to block traffic using outgoing ACLs. Outgoing ACLs do not

support the keyword “fragment” and will ignore it. If the keyword is included in the ACL, fragmented packets are not evaluated against the associated rules, possibly bypassing the security policy.

- **Cisco Fragment Keyword Outgoing Access Control Vulnerability**
  A vulnerability in IOS on Cisco 12000 series routers could let a remote user send unauthorized packets to a protected network. IOS for the Cisco 12000 has only recently added the ability to filter fragmented packets in outgoing traffic. If a ‘fragment’ rule in an outgoing ACL exists in a version without this feature, attackers could send fragmented packets to a protected network, thereby bypassing security policy.

- **Cisco 12000 Series Turbo ACL Fragment Bypass Vulnerability**
  A vulnerability in IOS on Cisco 12000 series routers could let a remote user send unauthorized packets to a protected network. The keyword ‘fragment’ in a compiled (turbo) ACL is ignored when evaluating packets that are addressed to the router itself.

- **Ntpd Remote Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in the Network Time Protocol (NTP) could let a remote user gain root access, execute arbitrary code, or cause a denial of service. NTP is used to synchronize the time between a computer and another system or time reference, using UDP as a transport protocol. There are two protocol versions in use, NTP v3 and NTP v4. The ntp daemon implementing version 3 is called xntp3, and the version implementing version 4 is called ntp.

- **Cisco IOS OSPF Neighbor Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in Cisco IOS when handling OSPF (Open Shortest Path First) packets could result in a denial of service or the execution of malicious code. Vulnerable versions are affected whenever more than 255 OSPF neighbors are announced.

- **Cisco IOS ICMP Redirect Routing Table Modification Vulnerability**
  A vulnerability in the Cisco IOS routing table could let remote users modify the table. If IP routing is disabled on a vulnerable router, the router will accept malicious ICMP redirect packets and modify its routing table accordingly. ICMP redirect messages are normally sent to indicate inefficient routing, a new route, or a routing change. A malicious user could specify a default gateway on the local network that does not exist, thus denying service to the affected router for traffic destined to any location outside the local subnet.

- **Cisco IOS EIGRP Announcement ARP Denial Of Service Vulnerability**
  A vulnerability in Cisco IOS allows spoofed EIGRP announcements to be sent via unicast. A neighbor announcement that is received by routers on a given network segment will cause an address resolution protocol (ARP)

storm, filling network capacity while routers attempt to contact the announcing neighbor and resulting in a denial of service. Additionally, resources on the router will become bound while the router attempts to reach the announcing neighbor.

- **IBM Lotus Domino HTTP Redirect Buffer Overflow Vulnerability**
  A buffer overflow vulnerability when IBM Lotus Domino 6 constructs an HTTP redirect response could let malicious clients gain control of the server. This vulnerability is reportedly fixed in Notes/Domino release 6.0.1.
- **Lotus Domino iNotes s_ViewName/Foldername Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in IBM Lotus Domino iNotes Web server when handling client-supplied request parameters could allow the execution of malicious code. This vulnerability is reportedly fixed in Lotus Domino 6.0.1.
- **IBM Lotus Domino Web Server HTTP POST Denial Of Service Vulnerability**
  A vulnerability in IBM Lotus Domino server could result in a denial of service. Specially crafted POST requests can cause the server to behave in an unpredictable manner.
- **Lotus Domino NSF Banner Information Disclosure Vulnerability**
  A vulnerability in IBM Lotus Domino server with DominoNoBanner set to a value of 1 could let remote users discover information about the layout of the file system. When a non-existent NSF database is requested, sensitive banner information could be disclosed.
- **Lotus Domino HTTP Authentication Logging Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in IBM Lotus Domino could let a remote user corrupt sensitive regions of memory with attacker-supplied values and possibly execute arbitrary code. This can occur because of insufficient bounds checking when HTTP Authentication data is logged to the DOMLOG.NSF database.
- **Lotus Domino MS-DOS Device Path Disclosure Vulnerability**
  A vulnerability in IBM Lotus Domino could give a remote user access to sensitive path information. Using specially crafted requests for MS-DOS devices could reveal information that could aid the attacker in further attacks. This issue was reported for Lotus Domino v5.0.9a on Microsoft Windows. Earlier versions may also be affected.
- **Lotus Domino Banner Information Disclosure Vulnerability**
  A vulnerability in IBM Lotus Domino server with NoBanner set to 1 could let a malicious user view the full path to the Web root. If a user submits an HTTP request for a non-existent Perl script, the server may return a 500

error page containing the full path of the file and possibly other system information.

- **Lotus Domino MS-Dos Device Name Denial Of Service Vulnerability**
  A vulnerability in IBM Lotus Domino server could be exploited for a denial of service. Invoking MS-DOS devices (such as CON, AUX, PRN, etc.) in multiple Web requests could halt service, requiring a manual restart to regain normal functionality.
- **Lotus Domino Remote Authentication Bypass Vulnerability**
  A vulnerability in IBM Lotus Domino server could let a malicious user bypass the authentication process. If a remote request for the file is submitted with a maliciously constructed file name, the authentication process may be bypassed. This issue is reportedly fixed in Domino 5.0.9.
- **Lotus Domino DOS Device Extension Denial of Service Vulnerability**
  A vulnerability in versions of IBM Lotus Domino server prior to 5.0.9a running on Windows 2000 could be exploited for a denial of service. If a request for a DOS device from CGI-BIN has an extension of 220 characters, the server executes a cmd.exe session to run nul.pif. The server will launch a pop-up window asking for a program association with which to run nul.pif. If this is done approximately 400 times, the server runs out of working threads thus causing a denial of service.
- **Lotus Domino Username Enumeration Vulnerability**
  A vulnerability in IBM Lotus Domino server could let remote users determine the validity of a user name existing on a host. If a remote user submits a GET request for a user account, the server returns an HTTP 200 OK message when given a valid user name. If the user name is not valid, a 404 File not Found error message is returned.
- **Embedded Web server identified**
  Embedded Web servers are usually found in network hardware such as routers, switches, and wireless access points. An attacker could discover an exploit or guess the password and gain access to the device, and thus be able to reconfigure or disable the device.
- **Wireless Access Point identified**
  The configuration interface of a wireless access point could allow unauthorized access to your network.
- **D-Link Wireless Access Point Identified**
  A D-link wireless access point could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities.

- **Netgear Wireless Access Point Identified**
  A Netgear wireless access point could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities.
- **Linksys Wireless Access Point Identified**
  A Linksys wireless access point could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities.
- **SMC Wireless Access Point Identified**
  An SMC wireless access point could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities.
- **Cisco-Aironet Wireless Access Point Identified**
  A Cisco-Aironet wireless access point could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities.
- **Cisco-Aironet Wireless Access Point Identified via SNMP**
  A Cisco-Aironet wireless access point via SNMP could reveal sensitive vendor information. Vendor information can assist an attacker in discovering default login credentials or known vulnerabilities. SNMP is also considered an insecure protocol.
- **Embedded Web server in device is vulnerable to Cross-Site Scripting**
  A vulnerability in a device running a ZyXel-RomPager Web server could let a malicious user gain unauthorized administrative access to the router (cross-site scripting attack). An attacker who knows the internal IP address of the router could execute arbitrary script code and possibly steal cookie-based authentication credentials from a user who has access to the administrative interface.
- **Allegro RomPager Malformed URL Request DoS Vulnerability**
  A vulnerability in Allegro RomPager could be exploited for a denial of service. A specifically-malformed request that is sent to RomPager could disable the device and possibly the parent device as well.

Current installation of Microsoft Jet database engine

Microsoft Data Access Components (MDAC) versions 2.6 and 2.7 do not include Microsoft Jet, Microsoft Jet OLE DB Provider, and the ODBC Desktop Database Drivers.

Symantec NetRecon requires these Microsoft Jet components to function properly. If you do not have the latest Jet components, you might get the following error message:

"Symantec NetRecon cannot connect to the database it uses to store information. A Windows NT Service Pack or application installation may have overwritten the Microsoft Database Access Components required by Symantec NetRecon. Please reinstall NetRecon. If reinstalling the product does not resolve this problem, contact your Symantec NetRecon customer support representative."

To solve this problem, install the latest Jet database engine. For more information on this issue and for instructions on installing the latest Jet database engine, see http://support.microsoft.com/default.aspx?scid=kb;EN-US;271908.

Integration with Symantec Enterprise Security Manager

Symantec NetRecon customers who also use Symantec ESM can detect vulnerabilities using the remote registry service. To take advantage of this functionality, the Enterprise Security Agent Service must be configured to run using an account that is part of the Domain Admins group rather than the Local System account.

To change the Enterprise Security Agent account

1. Access the Services control panel by clicking on the Windows **Start** button and selecting **Settings > Control Panel > Administrative Tools > Services**.
2. Find **Enterprise Security Agent** in the list of Windows Services.
3. Right-click on **Enterprise Security Agent** and select **Properties**.
4. Select the **Log On** tab.
5. Select the **This account** radio button.
6. Enter the name and password for an account that is in the Domain Admins group.
7. Click **OK**.
8. Right-click on **Enterprise Security Agent** and select **Restart**.

Cisco vulnerabilities

All of the Cisco vulnerabilities are currently detected via the SNMP service. Please ensure that the SNMP service is running on your Cisco devices. You will also need to add your read-only community strings, (if they are not already there) to c:\Program Files\Symantec\Netrecon 3.6\nrsnmpnames.inf if you want to detect your Cisco switches and routers successfully. If enabling SNMP presents a security risk, you can disable it after your scan is finished.

802.11x Wireless vulnerabilities

All of the wireless vulnerabilities are detected through your internal network. It is not required to purchase a wireless card in order to detect these vulnerabilities. The wireless access points will be detected based on whether the administrative web interface is enabled (usually TCP port 80). The main goal is to ensure that users have not plugged in a wireless access point into your corporate network thus exposing your network physically to the outside or airwave rage.

Lotus Domino vulnerabilities

The Lotus Domino vulnerabilities are based on the web server advertising its version number in the HTTP banner. Even though it is not recommended to enable the server to display the version information, you can do it by editing the notes.ini file and adding DominoNoBanner=0. This setting is enabled by default in earlier versions.

Security Update 2

Symantec NetRecon 3.6 SU2 adds detection and reporting of four Microsoft SQL Server vulnerabilities and the sendmail header processing buffer overflow. Several SQL Server vulnerabilities have also been renamed.

New vulnerability detection

With the addition of SU2, Symantec NetRecon can now detect and report the following vulnerabilities:

- **Microsoft Windows 2000 ntdll.dll Buffer Overflow Vulnerability**
  The Windows ntdll.dll system component vulnerable to a buffer overrun when passed data from certain functions; remote code execution is possible. The Windows 2000 library ntdll.dll includes a function that does not perform sufficient bounds checking. The vulnerability is present in the RtlDosPathNameToNtPathName_U function and may be exploited through

other programs that use the library if an attack vector permits it. One of these programs is the implementation of WebDAV that ships with IIS. The vector allows for the vulnerability in ntdll.dll to be exploited by a remote attacker.

- **Microsoft Data Access Components RDS Buffer Overflow Vulnerability**
  MDAC contains a buffer overflow that could lead to arbitrary code execution in MSIE and on vulnerable IIS servers.
- **Microsoft Windows Locator Service Buffer Overflow Vulnerability**
  The Locator service for Windows domain controller systems is prone to a buffer overflow condition. Arbitrary code execution is possible.
- **Microsoft SQL Server 2000 SQLXML Buffer Overflow Vulnerability**
  Attackers can initiate SQL Server 2000 buffer overflows by connecting to a host through HTTP, then submitting malformed data directly to the SQLXML HTTP component. The overflow condition occurs when an overly long value is given to the contenttype=parameter.
- **Microsoft SQL Server 2000 SQLXML Script Injection Vulnerability**
  SQLXML components are prone to script injection attacks via an unchecked parameter in XML tags. Under some circumstances it is possible to inject arbitrary script code in XML tags. This lets an attacker execute script code in the context of the Internet Explorer Security Zone associated with the IIS server running the vulnerable components.
- **Microsoft SQL Server 2000 lets remote attackers mount a DoS**
  SQL Server 2000 lets remote attackers mount a denial of service attack through a malformed 0x08 packet that is missing a colon separator.
- **Microsoft SQL Server 2000 OpenDataSource buffer overflow**
  Buffer overflow in the OpenDataSource function of the Jet engine on SQL Server 2000 lets remote attackers execute arbitrary code.
- **Sendmail Header Processing Buffer Overflow Vulnerability**
  A buffer overflow vulnerability in the SMTP header-parsing component of sendmail (versions 5.2 through 8.12.7) could let malicious users gain control of the server. This vulnerability could be exploited locally if the sendmail binary is setuid/setgid.

Vulnerability name changes

In SU2 the following Symantec NetRecon vulnerability names are changed:

Old name	New name
SQL Server 7.0 Remote Data Source function contains unchecked buffers	Microsoft SQL Server 7.0 OLE DB Provider Name Buffer Overflow

Old name	New name
SQL Server 2000 Remote Data Source function contains unchecked buffers	Microsoft SQL Server 2000 OLE DB Provider Name Buffer Overflow Vulnerability
SQL 7.0 extended stored procedures vulnerable to buffer overflow and DoS	Microsoft SQL Server 7.0 Multiple Extended Stored Procedure Buffer Overflow
SQL 2000 extended stored procedures vulnerable to buffer overflow and DoS	Microsoft SQL Server 2000 Multiple Extended Stored Procedure Buffer Overflow
SQL 2000 password encryption procedure vulnerable to buffer overflow attacks	Microsoft SQL Server 2000 Password Encrypt Procedure Buffer Overflow
SQL 2000 Resolution Service allows remote DoS or execution of arbitrary code	Microsoft SQL Server 2000 Resolution Service Heap Overflow Vulnerability
SQL Server 2000 sp_MScopyscript stored procedure fails to validate input	Microsoft SQL Server 2000 sp_MScopyscript stored procedure validation
SQL Server 7.0 authentication engine vulnerable to buffer overflow attacks	Microsoft SQL Server 7.0 authentication engine vulnerable to buffer overflow
Server 2000 authentication engine vulnerable to buffer overflow attacks	Microsoft SQL Server 2000 authentication engine vulnerable to buffer overflow
MSSQL Buffer Overflow vulnerable to W32.Slammer worm attack	Microsoft SQL Server 2000 Resolution Service Stack Overflow Vulnerability

Security Update 1

Symantec NetRecon 3.6 Security Update 1 (SU 1) contains corrected vulnerability names and command line interface (CLI) enhancements.

New vulnerability detection

Note: The names of SU 1 vulnerabilities were changed in SU2. The current (SU2+) names are used below. For the names that were used in SU 1, see "Vulnerability name changes" on page 188.

- **Microsoft SQL Server 7.0 OLE DB Provider Name Buffer Overflow Vulnerability**
  Symantec NetRecon can identify a buffer overflow in Microsoft SQL 7.0 that may let remote attackers execute arbitrary code on the system or gain privileged access to the SQL database.

- **Microsoft SQL Server 2000 OLE DB Provider Name Buffer Overflow Vulnerability**
  Symantec NetRecon can identify a buffer overflow in Microsoft SQL 2000 that may let remote attackers execute arbitrary code on the system or gain privileged access to the SQL database.
- **Microsoft SQL Server 7.0 Multiple Extended Stored Procedure Buffer Overflow**
  Symantec NetRecon can identify Microsoft SQL Server 7.0 extended stored procedures that fail to validate input correctly, which may allow buffer overflow attacks and denial of service (DoS) attacks.
- **Microsoft SQL Server 2000 Multiple Extended Stored Procedure Buffer Overflow**
  Symantec NetRecon can identify Microsoft SQL Server 2000 extended stored procedures that fail to validate input correctly, which may allow buffer overflow attacks and denial of service (DoS) attacks.
- **Microsoft SQL Server 2000 Password Encrypt Procedure Buffer Overflow**
  Symantec NetRecon can identify a Microsoft SQL Server 2000 credential encryption procedure that is vulnerable to a buffer overflow attack, which could compromise control of the database and possibly the server. The SQL 2000 Resolution Service may allow remote DoS or execution of arbitrary code.
- **Microsoft SQL Server 2000 Resolution Service Heap Overflow Vulnerability**
  Symantec NetRecon can identify the Microsoft SQL Server 2000 Resolution Services that contain multiple vulnerabilities. These vulnerabilities allow denial of service attacks as well as possible execution of arbitrary code through buffer overflow attacks.
- **Microsoft SQL Server 2000 sp_MScopyscript stored procedure validation**
  Symantec NetRecon can identify the Microsoft SQL Server 2000 sp_MScopyscript on network resources. Microsoft SQL Server 2000 fails to validate input, which may allow attackers to execute arbitrary code and gain privileged access to stored procedures in the SQL database.
- **Microsoft SQL Server 7.0 authentication engine vulnerable to buffer overflow**
  Symantec NetRecon can identify the authentication engine for the Microsoft SQL Server 7.0. The authentication engine is vulnerable to buffer overflow attacks that may let attackers execute arbitrary code and gain privileged access to the stored procedure, or cause a denial of service for the SQL service.

- **Microsoft SQL Server 2000 authentication engine vulnerable to buffer overflow**
  Symantec NetRecon can identify the authentication engine for the Microsoft SQL Server 2000. The authentication engine is vulnerable to buffer overflow attacks that may let attackers execute arbitrary code and gain privileged access to the stored procedure, or cause a denial of service for the SQL service.
- **Microsoft SQL Server 2000 Resolution Service Stack Overflow Vulnerability**
  Symantec NetRecon can identify a problem with the Microsoft SQL Server 2000 Resolution Service, which may make it possible for a remote user to execute arbitrary code on a vulnerable host. An attacker could exploit a stack-based overflow in the Resolution Service by sending a maliciously crafted UDP packet to port 1434. A vulnerable version of Microsoft SQL Server 2000 Desktop Engine is automatically installed with Internet Explorer 6 on .NET servers.
- **MSSQL Server detected**
  MSSQL Server has been detected.

Command line interface (CLI) enhancements

License key

The Symantec NetRecon command line interface (CLI) can now accept license key information. Four options are required to successfully register the license key using the CLI.

Option	Description
-license [-l]	Specify the Symantec NetRecon license key.
-company [-c]	Specify the company name that is associated with the license.
-serial [-s]	Specify the serial number that is associated with the license.
-type [-t]	Specify the type that is associated with the license.

Note: If an error occurs during the license registration, Symantec NetRecon places an error message in the errors.log file.

Symantec NetRecon data (.nrd) files

You must now use the following options to specify .nrd files in the command line interface.

Option	Description
-nrdin [-i]	Specify the .nrd input file.
-nrdout [-o]	Specify the .nrd output file.

Note: It is not necessary to submit .nrd files to change the license. However, if you omit one or both or the .nrd files, Symantec NetRecon will not attempt a scan.

CLI formatting and syntax are fully documented in the Symantec NetRecon online Help system. Users who are not familiar with the CLI should read the entire Use the Command Line Interface (CLI) Help section.

To locate the Help Topic on .nrd files

1. On the NetRecon console menu, click **Help**.
2. Click **Help Topics**.
3. Click the topic labeled **How do I...**
4. Click **Use the Command Line Interface (CLI)**.
5. Click **Understanding .NRD Files**.