

Symantec NetRecon™ 3.6
Security Update 20
Release Notes



Symantec NetRecon Security Update 20 Release Notes

The software that is described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
Documentation version: v3.6 040802

Copyright Notice

Copyright © 2004 Symantec Corporation.
All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks, and Symantec NetRecon, Symantec Enterprise Security Architecture, Symantec Enterprise Security Manager, LiveUpdate, and Symantec Security Response are trademarks of Symantec Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other product names that are mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
Printed in the United States of America.

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.

Revision February 21, 2001

Contents

NetRecon Security Update Release Notes

Security Update 20	11
New Vulnerability detection	11
Security Update 19	13
New Vulnerability detection	13
Security Update 18	20
New Vulnerability detection	20
Enhanced vulnerability detection	22
Security Update 17	24
Security Update 16	25
New vulnerability detection	25
Security Update 15	29
New vulnerability detection	29
Enhanced vulnerability detection	30
Security Update 14	31
New vulnerability detection	31
Security Update 13	34
New vulnerability detection	34
Security Update 12	37
New vulnerability detection	37
Security Update 11	38
New vulnerability detection	38
Security Update 10	41
Updated vulnerability detection	41
Security Update 9	41
Product enhancement	41
New vulnerability detection	42
Security Update 8	44
New vulnerability detection	44
Security Update 7	45
New objectives	45
New vulnerability detection	45
Security Update 6	46
New objectives	46
Known issues	46
New state detection	47

New vulnerability detection	47
Security Update 5	63
New vulnerability detection	63
Security Update 4	63
New vulnerability detection	63
Security Update 3	71
New vulnerability detection	71
Current installation of Microsoft Jet database engine	80
Integration with Symantec Enterprise Security Manager	80
Cisco vulnerabilities	81
802.11x Wireless vulnerabilities	81
Lotus Domino vulnerabilities	81
Security Update 2	81
New vulnerability detection	81
Vulnerability name changes	82
Security Update 1	83
New vulnerability detection	83
Command line interface (CLI) enhancements	85

NetRecon Security Update Release Notes

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 achieved 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 structure, 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 reported 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 DistributedDirector.

- **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_getvfsw 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 than 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/cgi-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 Announcement 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 initialize dynamically allocated data, which may be 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 than 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 42.)

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_error()` 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 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 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 range.

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_MScoptscript stored procedure fails to validate input	Microsoft SQL Server 2000 sp_MScoptscript 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 82.

- 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
-nrdir [-i]	Specify the .nrd input file.
-nrdir [-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**.