

Symantec NetRecon™ 3.6
Security Update 5
Release Notes



Symantec NetRecon Security Update 4 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 SU4

Copyright Notice

Copyright © 2003 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 US registered trademarks, and Symantec NetRecon, 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 agreements may contact Platinum Technical Support by 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

Release Notes

Security Update 5

New vulnerability detection	7
Corega Wireless Access Point Identified.....	7
IOData Wireless Access Point Identified	7
Melco Wireless Access Point Identified	7
Melco Wireless Access Point Identified via SNMP	7

Security Update 4

New vulnerability detection	8
Samba vulnerabilities	8
Samba call_trans2open Remote Buffer Overflow Vulnerability.....	8
Samba Multiple Unspecified Remote Buffer Overflow Vulnerabilities .	8
Samba-TNG Unspecified Remote Privilege Escalation Vulnerability....	8
Samba SMB/CIFS Packet Assembling Buffer Overflow Vulnerability ...	8
Samba REG File Writing Race Condition Vulnerability.....	8
Samba Server Encrypted Password Buffer Overrun Vulnerability.....	8
Samba Improperly Terminated Struct Buffer Overflow Vulnerability ..	9
Samba Remote Arbitrary File Creation Vulnerability.....	9
Samba Insecure TMP file Symbolic Link Vulnerability	9
Samba SWAT Symlink Vulnerability	9
Samba SWAT Logging Failure Vulnerability.....	9
Samba SWAT Logfile Permissions Vulnerability	9
Samba Pre-2.0.5 Vulnerabilities	9
Samba Long Password Buffer Overflow Vulnerability.....	10
Sendmail vulnerabilities	10
Sendmail Address Prescan Memory Corruption Vulnerability.....	10
Sendmail check_relay Access Bypassing Vulnerability	10
Sendmail Trojan Horse Vulnerability	10
Sendmail SMRSH Double Pipe Access Validation Vulnerability.....	10
Sendmail Long Ident Logging Circumvention Weakness.....	10
Sendmail DNS Map TXT Record Buffer Overflow Vulnerability	10
Sendmail File Locking Denial Of Service Vulnerability.....	11
Sendmail Inadequate Privilege Lowering Vulnerability.....	11
Sendmail Queue Processing Data Loss/DoS Vulnerability.....	11
Sendmail Debugger Arbitrary Code Execution Vulnerability	11

Sendmail Unsafe Signal Handling Race Condition Vulnerability	11
Sendmail ETRN Denial of Service Vulnerability	11
Sendmail Aliases Database Regeneration Vulnerability	12
MySQL vulnerabilities	13
MySQL Weak Password Encryption Vulnerability.....	13
MySQL mysqld Privilege Escalation Vulnerability	13
MySQL Double Free Heap Corruption Vulnerability	13
MySQL COM_CHANGE_USER Password Memory Corruption Vulnerabil- ity.....	13
MySQL COM_CHANGE_USER Password Length Account Compromise Vulnerability	13
MySQL libmysqlclient Library Read_Rows Buffer Overflow Vulnerability	13
MySQL libmysqlclient Library Read_One_Row Buffer Overflow Vulnerabil- ity.....	14
MySQL COM_TABLE_DUMP Memory Corruption Vulnerability	14
MySQL DataDir Parameter Local Buffer Overflow Vulnerability	14
MySQL Logging Not Enabled Weak Default Configuration Vulnerability	14
MySQL Null Root Password Weak Default Configuration Vulnerability	14
MySQL Bind Address Not Enabled Weak Default Configuration Vulnerabil- ity.....	14
MySQL Root Operation Symbolic Link File Overwriting Vulnerability	14
MySQL SHOW GRANTS Password Hash Disclosure Vulnerability....	15
MySQL Local Buffer Overflow Vulnerability.....	15
MySQL Unauthenticated Remote Access Vulnerability.....	15
MySQL Authentication Algorithm Vulnerability	15
MySQL GRANT Global Password Changing Vulnerability.....	15
Cisco vulnerabilities	15
Cisco Catalyst CatOS Authentication Bypass Vulnerability.....	15
Cisco Catalyst Unicast Traffic Broadcast Vulnerability.....	16
Cisco Catalyst ssh Protocol Mismatch Denial of Service Vulnerability	16
Cisco Catalyst Enable Password Bypass Vulnerability.....	16
Microsoft vulnerabilities	16
Microsoft Windows RPC Service Denial of Service Vulnerability.....	16
Microsoft IIS WebDAV Denial Of Service Vulnerability	16
New vulnerability detection	17
IE is vulnerable to arbitrary code injection through malformed header fields 17	
System Attendant on Exchange Server 2000 grants unauthorized registry ac- cess	17
Microsoft IE Arbitrary File Execution Vulnerability	17
Microsoft IE HTTP Request Encoding Vulnerability	17
Microsoft IE Zone Spoofing Vulnerability	17
Microsoft IE Arbitrary Program Execution Vulnerability	18

Microsoft IE Same Origin Policy Violation Vulnerability.....	18
Microsoft IE Forced Script Execution Vulnerability	18
VPN service enabled.....	18
Cisco IOS TFTP Server Long File Name Buffer Overflow Vulnerability	18
Cisco IOS ILMI SNMP Community String Vulnerability	19
Cisco IOS Malformed PPTP Packet Denial of Service Vulnerability ..	19
Multiple Vendor Session Initiation Protocol Vulnerabilities.....	19
Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability	19
Cisco Switch Router with Fast Ethernet Cards ACL Bypass/DoS Vulnerabili- ties	19
Cisco IOS Router Scan Software Reloading Vulnerability	19
Cisco Catalyst 802.1x Frame Forwarding Vulnerability.....	19
Cisco Catalyst Memory Leak Denial of Service Vulnerability	20
Cisco SSH Denial of Service Vulnerability.....	20
Cisco Local Interface ARP Denial of Service Vulnerability.....	20
Cisco IOS Cisco Express Forwarding Session Information Leakage Vulnera- bility	20
Cisco 12000 Series Internet Router Denial Of Service Vulnerability ..	20
Cisco Access Control List Fragment Non-blocking Vulnerability	20
Cisco 12000 Series Internet Router ACL Failure To Drop Packets Vulnerabil- ity.....	21
Cisco Outbound Access Control List Bypass Vulnerability	21
Cisco 12000 Outgoing ACL Fragmented Packet Vulnerability	21
Cisco Fragment Keyword Outgoing Access Control Vulnerability.....	21
Cisco 12000 Series Turbo ACL Fragment Bypass Vulnerability	21
Ntpd Remote Buffer Overflow Vulnerability	21
Cisco IOS OSPF Neighbor Buffer Overflow Vulnerability.....	22
Cisco IOS ICMP Redirect Routing Table Modification Vulnerability.	22
Cisco IOS EIGRP Announcement ARP Denial Of Service Vulnerability	22
IBM Lotus Domino HTTP Redirect Buffer Overflow Vulnerability....	22
Lotus Domino iNotes s_ViewName/Foldername Buffer Overflow Vulnera- bility.....	22
IBM Lotus Domino Web Server HTTP POST Denial Of Service Vulnerability	22
Lotus Domino NSF Banner Information Disclosure Vulnerability	23
Lotus Domino HTTP Authentication Logging Buffer Overflow Vulnerability	23
Lotus Domino MS-DOS Device Path Disclosure Vulnerability.....	23
Lotus Domino Banner Information Disclosure Vulnerability	23
Lotus Domino MS-Dos Device Name Denial Of Service Vulnerability	23
Lotus Domino Remote Authentication Bypass Vulnerability	23
Lotus Domino DOS Device Extension Denial of Service Vulnerability	23
Lotus Domino Username Enumeration Vulnerability	24

Embedded Web server identified.....	24
Wireless Access Point identified	24
D-Link Wireless Access Point Identified.....	24
Netgear Wireless Access Point Identified.....	24
Linksys Wireless Access Point Identified.....	24
SMC Wireless Access Point Identified.....	24
Cisco-Aironet Wireless Access Point Identified.....	24
Cisco-Aironet Wireless Access Point Identified via SNMP	25
Embedded Web server in device is vulnerable to Cross-Site Scripting.	25
Allegro RomPager Malformed URL Request DoS Vulnerability.....	25
Current installation of Microsoft Jet database engine	26
Integration with Symantec Enterprise Security Manager	26
Cisco vulnerabilities	27
802.11x Wireless vulnerabilities	27
Lotus Domino vulnerabilities	27
New vulnerability detection	28
Microsoft Windows 2000 ntdll.dll Buffer Overflow Vulnerability.....	28
Microsoft Data Access Components RDS Buffer Overflow Vulnerability	28
Microsoft Windows Locator Service Buffer Overflow Vulnerability ..	28
Microsoft SQL Server 2000 SQLXML Buffer Overflow Vulnerability	28
Microsoft SQL Server 2000 SQLXML Script Injection Vulnerability.	28
Microsoft SQL Server 2000 lets remote attackers mount a DoS	28
Microsoft SQL Server 2000 OpenDataSource buffer overflow.....	29
Sendmail Header Processing Buffer Overflow Vulnerability	29
Vulnerability name changes	29
New vulnerability detection	30
Microsoft SQL Server 7.0 OLE DB Provider Name Buffer Overflow Vulnerability	30
Microsoft SQL Server 2000 OLE DB Provider Name Buffer Overflow Vulnerability.....	30
Microsoft SQL Server 7.0 Multiple Extended Stored Procedure Buffer Overflow.....	30
Microsoft SQL Server 2000 Multiple Extended Stored Procedure Buffer Overflow.....	30
Microsoft SQL Server 2000 Password Encrypt Procedure Buffer Overflow	30
Microsoft SQL Server 2000 Resolution Service Heap Overflow Vulnerability	30
Microsoft SQL Server 2000 sp_MScoptscript stored procedure validation	31
Microsoft SQL Server 7.0 authentication engine vulnerable to buffer overflow	31
Microsoft SQL Server 2000 authentication engine vulnerable to buffer overflow.....	31
Microsoft SQL Server 2000 Resolution Service Stack Overflow Vulnerability	

31		
	MSSQL Server detected	31
	Command line interface (CLI) enhancements	32
	License key	32
	Symantec NetRecon data (.nrd) files	32

Release Notes

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 fifty-one new 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 vulnerabilities

- **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 smbmount 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 vulnerabilities

■ 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 vulnerabilities

■ 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 vulnerabilities

■ 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 vulnerabilities

■ **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:

Table 2-1 Vulnerability name changes

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
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

New vulnerability detection

Note: The names of SU1 vulnerabilities were changed in SU2. The current (SU2+) names are used below. For the names that were used in SU1, see [“Vulnerability name changes”](#) on page 29.

- **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_MSscopyscript stored procedure validation**
Symantec NetRecon can identify the Microsoft SQL Server 2000 sp_MSscopyscript 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.

Table 2-2 License key options

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.

Table 2-3 nrd file options

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 of 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**.

