

Symantec NetRecon™ Release Notes

Release for Symantec NetRecon 3.6



Symantec NetRecon™

Version 3.6 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 3.6

Copyright Notice

Copyright © 1995–2002 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, the Symantec logo, Symantec NetRecon, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and 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.

10 9 8 7 6 5 4 3 2 1

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 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 www-secure.symantec.com/platinum/.

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 CORPORATION SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION 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

New features and enhancements	9
Speed enhancements	9
Granular objective control	9
CVE mappings	10
Command Line Interface	10
All Security Updates since version 3.5	11
New vulnerability checks	11
Security Update 10	11
Security Update 9	13
Security Update 8	13
Security Update 7	14
Security Update 6	14
Security Update 5	16
Security Update 3	18
Security Update 2	23
Enhanced vulnerability checks	24
Security Update 8	24
New objectives	25
Security Update 7	25
Security Update 6	26
Security Update 5	26
Security Update 4	26
Security Update 1	27
Operating requirements	27
Frequently asked questions	28

Release Notes

This document includes the following topics:

- [New features and enhancements](#)
- [Operating requirements](#)

New features and enhancements

Symantec NetRecon™ version 3.6 includes significant speed enhancements, granular objective control, 296 CVE mappings, a better Command Line Interface, and Windows XP support, in addition to all Security Updates that were released after Symantec NetRecon version 3.5.

Speed enhancements

Before Symantec NetRecon version 3.5, SU8, when running a Symantec NetRecon scan, the engine would take 100 percent of the computer's CPU resources. In tests on computers meeting only the minimum hardware requirements for Symantec NetRecon, after installing version 3.6, Symantec NetRecon used less than 5 percent of the CPU resources.

The modifications affecting CPU usage have also improved Symantec NetRecon's run time. In tests, average run time was reduced 40 to 60 percent.

Granular objective control

Granular objectives let the user run certain commonly-used objectives individually, rather than as part of a full scan. This provides users with the versatility to select specific objectives from a predefined list. Because Symantec NetRecon runs only the necessary scans to obtain information about the selected objectives, users quickly have the needed information without running a full scan.

All objectives that were previously contained in the miscellaneous category, as well as certain objectives from the light, medium, and heavy scans, are part of the list of granular objectives. Those objectives from the light, medium, and heavy scans are still part of the full scans, and they run when a full scan is selected. Granular objectives cannot be run simultaneously with full scans or other granular objectives.

CVE mappings

Symantec NetRecon currently supports 296 CVE mappings. Internet links to relative CVE descriptions are included in the additional information section of each vulnerability.

Command Line Interface

The Symantec NetRecon Command Line Interface (CLI) lets scans run or spawn from other programs. The CLI provides important functionality in a number of different contexts.

Symantec NetRecon has several new CLI options that let users create reports in HTML format. Users can choose the format of the report and determine the report's content using options that select vulnerability, computer name, vulnerability risk by number, vulnerability risk by color, and other parameters.

Proper formatting and syntax is documented in the help files.

To locate Help files for the CLI

- 1 Open the Symantec NetRecon online Help files.
- 2 Click **How do I...**
- 3 Click **Use the Command Line Interface**.
- 4 Click the section titled **Understanding .nrd Files**.

Users who are not familiar with the CLI should read the entire Help section for using the command line interface to understand the complete command line syntax.

All Security Updates since version 3.5

New vulnerability checks

Security Update 10

Apache Web server chunk handling vulnerability

Symantec NetRecon can locate versions of Apache Web Server that may be vulnerable to a remote attack. Attackers can use specifically malformed chunk-encoded HTTP requests to execute arbitrary code on Apache servers.

PCAnywhere can provide remote access to a computer

Symantec NetRecon can find copies of PCAnywhere that are running on network resources. PCAnywhere is a program that allows remote control and access to a system. Unauthorized installations could pose a security risk.

PC Protect Stealth logs all activity and stores this in a local encrypted file

Symantec NetRecon can locate installations of PC Protect Stealth on network resources. Though PC Protect Stealth logs are encrypted, unauthorized access to the logs could provide an attacker with passwords and other sensitive information.

Netlook allows a remote capture of screenshots

Symantec NetRecon can locate installations of Netlook that are running on network resources. Netlook can provide an attacker with remote screen shots of a system. These screen shots can include sensitive information.

NetBus can be used as a backdoor program allowing remote access

Symantec NetRecon can locate installations of NetBus on network resources. NetBus is a backdoor program that lets unauthorized users remotely perform a variety of operations, such as changing the registry, executing commands, starting services, listing files, uploading or downloading files, or other malicious activities.

IKS will keep a log of all keystrokes typed

Symantec NetRecon can locate installations of IKS (Invisible Keylogger Stealth) on network resources. The IKS logs are typically held in a file called iks.txt or iks.dat. These files may be viewed to obtain passwords and other sensitive information. Unauthorized installations can pose a security risk.

Desktop Delivery can provide remote access to a computer

Symantec NetRecon can locate installations of Desktop Delivery on network resources. Desktop Delivery is a program that can allow remote control and access to a system.

CaptureScreen can provide remote access to a computer

Symantec NetRecon can locate installations of CaptureScreen on network resources. CaptureScreen is a program that can allow remote control and access to a system.

Carbon Copy can provide remote access to a computer

Symantec NetRecon can locate installations of Carbon Copy on network resources. Carbon Copy is a program that can allow remote control and access to a system.

Virtualized UNC Shares Vulnerability

Symantec NetRecon can discover a system vulnerability that allows source code to be sent to an attacker. When a virtual directory is mapped to a Universal Naming Convention (UNC) share, and a request for a file in the directory contains one of several particular characters at the end of the request, the expected Internet Server Application Programming Interface (ISAPI) extension processing may not occur. This can result in the source code version of the file being sent to the attacker's browser.

WebDAV Denial of Service Vulnerability

Symantec NetRecon can discover a WebDAV vulnerability that lets attackers overwhelm system resources, resulting in a denial of service. This vulnerability occurs when WebDAV mishandles certain very long, malformed requests. The final result causes an access violation and crashes the IIS 5.0 server.

Domain Controller Request Denial of Service

Symantec NetRecon can discover an NT service vulnerability that allows an attacker to overload system resources, resulting in a denial of service. An NT service that runs on all Windows 2000 domain controllers contains a flaw that affects how a system processes a certain type of invalid service request. If an attacker sends a continuous stream of these requests to an affected machine, the attempt to process the requests consumes most or all of the CPU capacity.

Security Update 9

Malformed RPC request can cause service problems

Symantec NetRecon can discover an RPC server vulnerability that allows denial of service attacks and could allow attackers to crash the server. Several of the RPC servers that are associated with Microsoft Exchange, SQL Server, Windows NT 4.0 and Windows 2000 services do not adequately validate inputs. In some cases, RPC servers accept invalid inputs that prevent normal processing. Specific input values vary from RPC server to RPC server, but an attacker can send malformed RPC packets to the system services to deny or crash the services.

Packaging anomaly could cause hotfixes to be removed

Symantec NetRecon can discover a missing patch for a packaging anomaly that allows Windows 2000 post-Service Pack 1 (SP1) hotfixes to be overwritten. Under certain circumstances, the Windows 2000 post-SP1 catalog file (Sp2.cat) may be incorrectly versioned. This causes it to replace a new version of Sp2.cat with an old one.

Denial of service in ISC BIND 9

Symantec NetRecon can discover a vulnerable version of BIND that allows remote attackers to shut down BIND servers. An attacker sends a DNS packet that is designed to trigger an internal consistency check. This check fails to properly handle the request, causing BIND to shut down.

Security Update 8

wu-ftpd format string debug set allows remote command execution

Symantec NetRecon can discover versions of wu-ftpd that are running on network resources which allow unauthorized users to create and run unauthorized commands on those resources.

Sendmail mail.local allows unauthorized LMTP commands to be executed

Symantec NetRecon can discover a Sendmail service that could allow unauthorized execution of LMTP (local mail transfer protocol) commands. The vulnerability is the result of a problem with mail.local, a program that is included with Sendmail, which was intended as a delivery agent for local mail using LMTP. In LMTP mode, mail.local checks user input for an end of message indicator. If an unauthorized user were to synthesize a false end of message indicator, mail.local would treat any text after the synthesized indicator as LMTP commands.

OpenSSH UseLogin directive can allow remote access as root

Symantec NetRecon can discover network resources with an OpenSSH server vulnerability that allows intruders to execute arbitrary code. If an intruder can authenticate to the system using public key authentication, and the UseLogin directive is enabled, the intruder can set environment variables that are used by login. Anyone exploiting this vulnerability can execute commands with the privileges of OpenSSH, which is usually root. UseLogin is not enabled by default, but it is a common configuration.

Security Update 7

Multiple buffer overflows in PHP allow remote access to server

Symantec NetRecon can discover network resources that are running Web servers and versions of PHP that are vulnerable to buffer overflow exploits.

PHP is a common scripting language that can be installed on Web servers such as Apache, IIS, Netscape, and others.

Vulnerabilities in the `php_mime_split` function may allow an intruder to execute arbitrary code with the privileges of the Web server. This vulnerability is detected based on the PHP version, which is obtained from the Web server banner.

Security Update 6

Universal Plug and Play Service Identified

Symantec NetRecon can discover a network resource that is running the Universal Plug and Play service by communicating with the Universal Plug and Play service to verify its existence. Disable the SSDP Discovery Service if it is not needed and block access to ports UDP 1900 and TCP 5000 at your firewalls and router ACLs.

Discover NSF vulnerabilities

Following is a list of the new NSF vulnerability checks:

- Use Windows networking
- Use Windows networking to discover vulnerabilities
- Obtain access to Windows network resources
- Discover vulnerabilities of Netware network resources
- Discover RPC services
- Obtain maps from NFS servers

- Discover SMB server vulnerabilities
- Discover SMTP vulnerabilities
- Discover FTP vulnerabilities
- Discover IRC vulnerabilities
- Discover HTTP vulnerabilities
- Discover finger vulnerabilities
- Discover BIND vulnerabilities
- Discover Oracle database vulnerabilities
- Trojans
- Discover trojans and vulnerable services running on UDP ports
- Discover trojans and vulnerable services running on TCP ports
- SNMP vulnerabilities
- Guess SNMP community names
- Discover SNMP vulnerabilities
- Discover SNMP vulnerabilities of identified SNMP agents
- Discover network resources that are not running Symantec Enterprise Security Manager agents
- Discover network resources that are not running Intruder Alert agents
- All TCP services (full connect)
- Discover all privileged TCP services (full connect)
- Discover all non-privileged TCP services (full connect)
- Discover select TCP services
- Discover select TCP and UDP services (half open)
- Discover all TCP and UDP services (half open)
- Obtain banners from TCP services
- Discover network resources that are running Norton AntiVirus Corporate Edition
- Discover network resources that are not running Norton AntiVirus Corporate Edition
- Enumerate resources

- Identify network resources
- Enumerate target network resources
- Use ICMP protocol to scan network resources
- Analyze resources to determine preliminary vulnerabilities

Security Update 5

Security Update 5 introduced five new vulnerability checks. Although versions of these checks already existed in the database, these checks go one step further in identifying not only the open port, but the particular trojan that is using the UDP protocol.

mstream trojan horse master allows attack-by-proxy

Symantec NetRecon can discover a network resource that is running an mstream trojan horse master.

mstream is a distributed attack tool that can be installed on compromised network resources by attackers who wish to use those network resources as attack agents in subsequent attacks. Placing mstream components allows attackers to use your bandwidth and computing resources to launch a wide range of denial of service attacks against other network resources.

The presence of mstream indicates that the network resource was compromised through another vulnerability.

mstream trojan horse server allows attack-by-proxy

Symantec NetRecon can discover a network resource that is running an mstream trojan horse server.

mstream is a distributed attack tool that can be installed on compromised network resources by attackers who wish to use those network resources as attack agents in subsequent attacks. Placing mstream components allows attackers to use your bandwidth and computing resources to launch a wide range of denial of service attacks against other network resources.

The presence of mstream indicates that the network resource was compromised through another vulnerability.

wintrino trojan horse daemon allows attack-by-proxy

Symantec NetRecon can discover a network resource that is running a wintrino trojan horse daemon.

Wintrinoo is a distributed attack tool that can be installed on compromised network resources by attackers who wish to use those network resources as attack agents in subsequent attacks. Placing wintrinoo components allows attackers to use your bandwidth and computing resources to launch a wide range of denial of service attacks against other network resources.

The presence of wintrinoo indicates that the network resource was compromised through another vulnerability. The registry method is subject to registry access being obtained, but it is unlikely to yield a false positive.

trinoo trojan horse daemon allows attack-by-proxy

Symantec NetRecon can discover a network resource that is running a trinoo trojan horse daemon.

Trinoo is a distributed attack tool that can be installed on compromised network resources by attackers who wish to use those network resources as attack agents in subsequent attacks. Placing trinoo components allows attackers to use your bandwidth and computing resources to launch a wide range of denial of service attacks against other network resources.

The presence of trinoo indicates that the network resource was compromised through another vulnerability.

shaft trojan horse daemon allows attack-by-proxy

Symantec NetRecon can discover a network resource that is running a shaft trojan horse agent.

Shaft is a distributed attack tool that can be installed on compromised network resources by attackers who wish to use those network resources as attack agents in subsequent attacks. Placing shaft components allows attackers to use your bandwidth and computing resources to launch a wide range of denial of service attacks against other network resources.

The presence of shaft indicates that the network resource was compromised through another vulnerability.

Security Update 3

Security Update 3 introduced 143 new Web server vulnerability checks such as vulnerable CGI script files, Cold Fusion files, and Active Server Page files. Each of these checks was previously located only in the Symantec ESM for WebServers 1.0 product.

Following is a list of the new Web server vulnerability checks:

- HTTP allows CGI access to .html/...../config.sys
- HTTP allows CGI access to _vti_bin/shtml.dll
- HTTP allows CGI access to _vti_inf.html
- HTTP allows CGI access to _vti_pvt/administrators.pwd
- HTTP allows CGI access to _vti_pvt/authors.pwd
- HTTP allows CGI access to _vti_pvt/service.grp
- HTTP allows CGI access to _vti_pvt/service.pwd
- HTTP allows CGI access to _vti_pvt/users.pwd
- HTTP allows CGI access to achg.htr
- HTTP allows CGI access to aexp.htr
- HTTP allows CGI access to aexp2.htr
- HTTP allows CGI access to aexp2b.htr
- HTTP allows CGI access to aexp3.htr
- HTTP allows CGI access to aexp4.htr
- HTTP allows CGI access to aexp4b.htr
- HTTP allows CGI access to anot.htr
- HTTP allows CGI access to anot3.htr
- HTTP allows CGI access to autoexec.bat
- HTTP allows CGI access to carbo.dll
- HTTP allows CGI access to config.sys
- HTTP allows CGI access to doc
- HTTP allows CGI access to etc/group
- HTTP allows CGI access to etc/passwd
- HTTP allows CGI access to iisadmin/bdir.htr

- HTTP allows CGI access to iisadmin/ism.dll
- HTTP allows CGI access to passwd
- HTTP allows CGI access to passwd.pwd
- HTTP allows CGI access to passwd.pwl
- HTTP allows CGI access to passwd.txt
- HTTP allows CGI access to password
- HTTP allows CGI access to password.pwd
- HTTP allows CGI access to password.pwl
- HTTP allows CGI access to password.txt
- HTTP allows execution of AT-admin.cgi CGI
- HTTP allows execution of AnyBoard.cgi CGI
- HTTP allows execution of AnyForm.cgi CGI
- HTTP allows execution of AnyForm2 CGI
- HTTP allows execution of CGIemail.exe CGI
- HTTP allows execution of Count.cgi CGI
- HTTP allows execution of FormHandler.cgi CGI
- HTTP allows execution of GetFile.cfm CGI
- HTTP allows execution of _AuthChangeUrl CGI
- HTTP allows execution of _vti_bin/shtml.exe CGI
- HTTP allows execution of _vti_pvt/shtml.exe CGI
- HTTP allows execution of adminlogin CGI
- HTTP allows execution of adsamples/config/site.csc CGI
- HTTP allows execution of aglimpse CGI
- HTTP allows execution of alibaba.pl|dir CGI
- HTTP allows execution of args.bat CGI
- HTTP allows execution of args.cmd CGI
- HTTP allows execution of ax-admin.cgi CGI
- HTTP allows execution of ax.cgi CGI
- HTTP allows execution of bb-hist.sh CGI

- HTTP allows execution of bigconf.cgi CGI
- HTTP allows execution of bnbform.cgi CGI
- HTTP allows execution of catalog_type.asp CGI
- HTTP allows execution of cgi-shl/win-c-sample.exe CGI
- HTTP allows execution of cgiwrap CGI
- HTTP allows execution of classifieds.cgi CGI
- HTTP allows execution of convert.bas CGI
- HTTP allows execution of counter.exe CGI
- HTTP allows execution of day5datacopier.cgi CGI
- HTTP allows execution of day5datanotifier.cgi CGI
- HTTP allows execution of default.asp CGI
- HTTP allows execution of dfire.cgi CGI
- HTTP allows execution of displayopenedfile.cfm CGI
- HTTP allows execution of domcfg.nsf CGI
- HTTP allows execution of dumpenv.pl CGI
- HTTP allows execution of edit.pl CGI
- HTTP allows execution of environ.cgi CGI
- HTTP allows execution of envout.bat CGI
- HTTP allows execution of exprcalc.cfm CGI
- HTTP allows execution of faxsurvey CGI
- HTTP allows execution of filemail.pl CGI
- HTTP allows execution of files.pl CGI
- HTTP allows execution of formmail.pl CGI
- HTTP allows execution of fpcount.exe CGI
- HTTP allows execution of fpexplore.exe CGI
- HTTP allows execution of gH.cgi CGI
- HTTP allows execution of glimpse CGI
- HTTP allows execution of guestbook.cgi CGI
- HTTP allows execution of guestbook.pl CGI

- HTTP allows execution of handler CGI
- HTTP allows execution of handler.cgi CGI
- HTTP allows execution of info2www CGI
- HTTP allows execution of input.bat CGI
- HTTP allows execution of input2.bat CGI
- HTTP allows execution of kcms_configure CGI
- HTTP allows execution of maillist.pl CGI
- HTTP allows execution of man.sh CGI
- HTTP allows execution of nph-publish CGI
- HTTP allows execution of nph-test-cgi CGI
- HTTP allows execution of openfile.cfm CGI
- HTTP allows execution of perl/files.pl CGI
- HTTP allows execution of perlshop.cgi CGI
- HTTP allows execution of pfdisplay.cgi CGI
- HTTP allows execution of pfieffer.bat CGI
- HTTP allows execution of pfieffer.cmd CGI
- HTTP allows execution of phf.cgi CGI
- HTTP allows execution of phf.pp CGI
- HTTP allows execution of php CGI
- HTTP allows execution of php.cgi CGI
- HTTP allows execution of ppscgi.exe CGI
- HTTP allows execution of queryhit.htm CGI
- HTTP allows execution of responder.cgi CGI
- HTTP allows execution of rquest.exe CGI
- HTTP allows execution of rwwwshell.pl CGI
- HTTP allows execution of s97_cgi CGI
- HTTP allows execution of s97r_cgi CGI
- HTTP allows execution of search.cgi CGI
- HTTP allows execution of search97.vts CGI

- HTTP allows execution of sendform.cgi CGI
- HTTP allows execution of sendmail.cfm CGI
- HTTP allows execution of showcode.asp CGI
- HTTP allows execution of startstop.html CGI
- HTTP allows execution of status.cgi CGI
- HTTP allows execution of survey.cgi CGI
- HTTP allows execution of test.bat CGI
- HTTP allows execution of textcounter.pl CGI
- HTTP allows execution of tools/getdrvs.exe CGI
- HTTP allows execution of tools/newdsn.exe CGI
- HTTP allows execution of tst.bat CGI
- HTTP allows execution of unlg1.1 CGI
- HTTP allows execution of unlg1.2 CGI
- HTTP allows execution of upload.pl CGI
- HTTP allows execution of uploader.exe CGI
- HTTP allows execution of view-source CGI
- HTTP allows execution of visadmin.exe CGI
- HTTP allows execution of w3-mysql CGI
- HTTP allows execution of webbbs.cgi CGI
- HTTP allows execution of webdist.cgi CGI
- HTTP allows execution of webgais CGI
- HTTP allows execution of webhits.exe CGI
- HTTP allows execution of websendmail CGI
- HTTP allows execution of webwho.pl CGI
- HTTP allows execution of wguest.exe CGI
- HTTP allows execution of whois_raw.cgi CGI
- HTTP allows execution of wrap CGI
- HTTP allows execution of wrap.cgi CGI
- HTTP allows execution of www-sql CGI

- HTTP allows execution of wwwadmin.pl CGI
- HTTP allows execution of wwwboard.cgi CGI
- HTTP allows execution of wwwboard.pl CGI

Security Update 2

Code Red II

Symantec NetRecon can discover a Microsoft IIS server that is infected with a variant of the Code Red worm, which is called Code Red II. Code Red and Code Red II are malicious programs that infect Microsoft IIS Web servers through a common indexing service vulnerability and then attempt to randomly propagate to other Microsoft IIS servers. Code Red II uses similar penetration and propagation techniques as the original Code Red worm by exploiting the Microsoft IIS indexing service. However, Code Red II also enables a backdoor that allows remote system level access.

Oracle TNS Listener contains a Buffer Overflow

Symantec NetRecon can discover a version of Oracle TNS listener that is susceptible to a buffer overflow attack. The Oracle TNS (Transparent Network Substrate) provides the ability to communicate with Oracle database services remotely. A bug in the TNS listener service allows a remote attacker to overflow a buffer and gain full control of the database services. On Microsoft Windows NT and Windows 2000, the TNS listener service has LocalSystem privileges that let a remote attacker gain control of the operating system as well as the database services. On UNIX platforms, a remote attacker may gain whatever privileges are owned by the oracle user account.

Microsoft IIS Server is vulnerable from superfluous decoding

Symantec NetRecon can discover a Microsoft IIS server that superfluously decodes URL characters that can lead to a remote intruder running arbitrary commands. Following RFC 2396 standards, Web servers will decode characters in a URI or URL that have been escaped and represented in a hexadecimal format. According to the RFC, characters may be escaped by the percent sign (%) followed by two hexadecimal digits representing the character. For example, the string 'A string in a URL' can be represented by 'A%20string in %61 URL.'

Security measures have been implemented within IIS to avoid remote intruders from escaping directory traversal characters i.e. './' and gaining access to files outside the Web server document root. However, because IIS decodes some of the input twice and security checks are applied only to the results of the first decoding, intruders are still able to arbitrarily access files on the volume. This can

be particularly dangerous when files such as 'cmd.exe' are accessed, as it allows the remote intruder to run commands on the IIS server.

Tomcat allows directory traversal

Symantec NetRecon can discover a Tomcat Java server that allows directory traversals. A remote user can view the contents of files outside of the document root directory by making HTTP requests with directory traversals in the URL. Disclosure of this type of information can provide remote intruders with possible vulnerabilities that they can exploit. It may also divulge privileged information that may compromise confidentiality.

Tomcat allows script source code disclosure

Symantec NetRecon can discover a Tomcat Java server that allows script source code to be disclosed by using URL escaped characters. A remote user can obtain the source code for JavaServer Pages by using URL encoding within an HTTP request, or by using a malformed HTTP request. Symantec NetRecon detects both of these exploit methods. Disclosure of this type of information can provide remote intruders with possible vulnerabilities that they can exploit.

Enhanced vulnerability checks

Security Update 8

Girlfriend backdoor detected

Symantec NetRecon can establish a positive communication with the Girlfriend backdoor trojan. Using TCP port 21554, Symantec NetRecon attempts to open a line of communication with the trojan, positively verifying its existence.

Possible Girlfriend backdoor detected

If Symantec NetRecon detects that the port that is commonly used by the Girlfriend backdoor trojan is in use, but Symantec NetRecon is unable to connect with the trojan, it will use this vulnerability check to identify a possible detection. This is identified as a possible detection because an unlikely possibility exists that a legitimate program is using that port.

SubSeven backdoor detected

Symantec NetRecon can establish a positive communication with the SubSeven backdoor trojan. Using a port commonly used by SubSeven, Symantec NetRecon attempts to open a line of communication with the trojan, positively verifying its existence.

Possible SubSeven backdoor detected

If Symantec NetRecon detects that a port that is commonly used by the SubSeven backdoor program is in use, but Symantec NetRecon is unable to connect with the program, it will use this vulnerability check to identify a possible detection. This is identified as a possible detection because an unlikely possibility exists that a legitimate program is using that port.

New objectives

Security Update 7

The following two objectives are enhanced:

- To discover network resources that are not running Norton AntiVirus Corporate Edition
- To discover network resources that are running Norton AntiVirus Corporate Edition

For both objectives, an additional default port (port 3837) for NAVCE (Norton Antivirus Corporate Edition) detection has been included.

The ability for users to scan ports for NAVCE, in addition to the default port, has been added. This is accomplished by adding entries to the modules.inf in the ~/Symantec/NetRecon 3.5/ directory.

Note the following examples:

- To discover network resources that are not running Norton AntiVirus Corporate Edition on ports 1111, 2222, and 3333 (no spaces between port numbers)


```
R Name="Discover network resources not running Norton AntiVirus Corporate Edition" Parent="Miscellaneous" Command="navce -x -t 1000 -C 1111,2222,3333" Met="R Vulnerability=!*" Source=!navce -x!" Filter="R .List=!NI!" Try="Identify network resources"
```
- To discover network resources that are running Norton AntiVirus Corporate Edition on ports 1111, 2222, and 3333 (no spaces between port numbers).


```
R Name="Discover network resources running Norton AntiVirus Corporate Edition" Parent="Miscellaneous" Command="navce -t 1000 -C 1111,2222,3333" Met="R Vulnerability=!*" Source=!navce!" Filter="R .List=!NI!" Try="Identify network resources"
```

By default the user should use the -C option that is used as part of the “navce -t 1000 -C <port>” command. If there is still difficulty in detecting older versions of NAVCE, the -s option may be used instead.

Security Update 6

Discover trojans and vulnerable services running on UDP ports

This objective can discover trojans and vulnerable services that are using the UDP protocol by communicating with them on their own ports in addition to determining that the port is open. This avoids false positives from benign processes that are using a port that is known to be used by some trojans and vulnerable services.

Discover trojans and vulnerable services running on TCP ports

This objective can discover trojans and vulnerable services that are using the TCP protocol by communicating with them on their own ports in addition to determining that the port is open. This avoids false positives from benign processes that are using a port that is known to be used by some trojans and vulnerable services.

Security Update 5

Discover trojans running on UDP ports

This objective can discover trojans that are using the UDP protocol by communicating with them on their own ports in addition to determining that the port is open. This avoids false positives from benign processes that are using a port that is known to be used by some trojans and vulnerable services.

Security Update 4

Discover network resources not running Norton AntiVirus Corporate Edition

This objective reports only messages for machines where NAVCE is found on the machine and displays the message, "NAVCE Service Identified." This objective checks for the following information:

Service:	NAVCE Client or NAVCE Server
Version/Revision:	NAVCE version number Symantec supports only NAVCE versions 6.x or newer.
Miscellaneous:	Date and time of "Last Virus Definition" and date and time of "Last System Scan"

Discover network resources running Norton AntiVirus Corporate Edition

This objective reports only messages for machines where NAVCE is not detected on the machine and displays the message, “NAVCE service not detected.”

If you specify an IP address or machine name that is not valid, Symantec NetRecon generates a service not detected message.

Security Update 1

IIS Indexing Service exposure may allow remote compromise

This objective can discover whether a Microsoft IIS server has Indexing Service extension script mappings (.ida and .idq) enabled. The Indexing Service is known to be vulnerable to at least one buffer overflow exploit (Code Red worm) that allows complete compromise. This check determines if the .ida and .idq script extensions have been unmapped on the IIS server. The Indexing Service should be unmapped (via the Internet Services Manager in IIS) unless there is a business need.

Operating requirements

Minimum system requirements to run Symantec NetRecon version 3.6 are listed in the following table:

Table 1-1 Minimum system requirements

System Variables	Minimum Requirements
Operating system	Windows NT 4 (Workstation or Server) with Service Pack 6 or greater, Windows 2000, and Windows XP
Memory	96 MB
Disk space	40 MB
Display	VGA
CPU	Pentium-class or greater

This product release may run on newer versions of the supported operating systems, but Symantec reserves the right to certify the release on the new versions.

Operating requirements for all products, including Symantec NetRecon, are located on the Internet at:

<http://www.symantec.com/techsupp/> > Enterprise > Symantec NetRecon, version # > Supported Configurations

Frequently asked questions

- Where can I find the Security Update software?
Download the appropriate software for your system architectures from the Symantec Web site at: <http://securityresponse.symantec.com/>
Click **Security Updates: NetRecon**
- How do I install the Security Update release?
Security Updates are self-extracting executables that, when executed, run a setup program.

To install the Security Update:

- 1 Double-click the icon in the Windows Explorer.
- 2 Select **Start > Run**.
- 3 Click **Browse**.
- 4 Locate the Security Update executable.
- 5 Click **Open**.
- 6 Click **OK**.
- 7 Follow the prompts in the setup program.
If Symantec ESM is installed on your system and Symantec NetRecon detects it, you will be prompted for the user name, password, and name of the Symantec ESM manager after the files are copied.