

Release Notes

Symantec NetRecon™

Version 3.5 Security Update 9





The information in this document is subject to change without notice and must not be construed as a commitment on the part of Symantec. Symantec assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such a license.

No part of this documentation may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means—graphic, electronic, or mechanical, including photocopying and recording—without the prior written permission of the copyright owner.

© 1995-2002 Symantec Corporation.

All rights reserved.

Printed in the United States of America.

CONFIDENTIAL AND PROPRIETARY INFORMATION OF SYMANTEC CORPORATION.

Additional copies of this document or of other Symantec publications may be ordered from your Symantec account manager.

Customer Support United States:	Phone:	(888) 727-8671
	Fax:	(801) 227-3788
	Web:	http://www.symantec.com/techsupp

Global Customer Support:	Phone:	+44 (0) 1372 214321
	Fax:	+44 (0) 1372 214341
	Web:	http://www.symantec.com/globalsites.html

Licensing Issues:	Phone:	(888) 727-8671
	Fax:	(781) 890-6532
	E-mail:	license@symantec.com

Trademarks

Symantec is a registered trademark of Symantec, Inc.; NetRecon and the Symantec logo are trademarks of the same company registered in the United States of America and certain other countries. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other brands and product names are trademarks, or registered trademarks, of their respective companies.

Document Revised: June 2002

Release **Notes**

Description

Symantec NetRecon 3.5 Security Update 9 is a content update for Symantec NetRecon 3.5 that introduces three new vulnerability checks: a check for identifying an RPC server vulnerability, a check for a missing Windows 2000 patch that fixes a packaging anomaly, and a check for a vulnerability in ISC BIND 9 that allows a denial of service attack.

Security Update 9 also adds new functionality to NetRecon that lets users select granular objectives. These objectives run individually, rapidly providing needed information to users.

The Security Update installation adds several new files to the NetRecon directory and modifies several other files. Security Update 9 includes all changes that were made in previous NetRecon 3.5 Security Updates.

Installing

Security Update 9 is installed completely through LiveUpdate. You cannot update the product with an executable.

LiveUpdate can be started from the LiveUpdate button in the NetRecon icon bar or the Help menu bar. Click and follow the instructions.

Verifying Installation

To verify installation, go to Help/About and confirm that the version is 3.5 SU9.

Security Update 9

New Vulnerability Checks

Malformed RPC request can cause service problems

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

NetRecon can discover a missing patch for a packaging anomaly that allows Windows 2000 post-SP1 hotfixes to be overwritten. Under certain circumstances, Windows 2000 post-Service Pack 1 (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

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.

New Features and Enhancements

Granular objectives

NetRecon has added several granular objectives to give users an ability to run certain commonly-used objectives individually, rather than as part of a full scan. This enhancement gives users the versatility to select specific objectives from the list. Because NetRecon runs only the necessary scans to obtain information regarding the selected objectives, rather than running a full scan, users quickly have the needed information.

All objectives 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 have parent and child objectives. Select a parent objective to run each of the child objectives, or select a child objective to run it individually. In the list of granular objectives, indented items are child objectives.

- ◆ Discover NSF vulnerabilities
- ◆ 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

Granular objectives cannot be run simultaneously with full scans or other granular objectives.

Security Update 8

New Vulnerability Checks

wu-ftpd format string debug set allows remote command execution

NetRecon can discover versions of wu-ftp 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

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 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. Should an unauthorized user 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

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; however, it is a common configuration.

Enhanced Vulnerability Checks

Girlfriend backdoor detected

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

Possible Girlfriend backdoor detected

If NetRecon detects that the port commonly used by the Girlfriend backdoor trojan is in use, but NetRecon is unable to connect with the trojan, it will use this vulnerability check identifying 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

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

Possible SubSeven backdoor detected

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

New Features and Enhancements

Speed and performance

NetRecon's speed and performance have been dramatically improved with Security Update 8. Formerly, when running a NetRecon scan, the engine would take 100 percent of the computer's CPU resources. In tests, on machines meeting only

the minimum hardware requirements for NetRecon, after installing Security Update 8, NetRecon used less than 5 percent of the CPU resources.

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

Uninstall improvement

NetRecon's uninstall capability has also been enhanced. Uninstall now recognizes and removes files added to NetRecon via the Security Updates after the original installation of version 3.5.

Security Update 7

New Objectives

The following are enhancements to the following two objectives:

- ◆ To discover network resources not running Norton AntiVirus Corporate Edition
- ◆ To discover network resources 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 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 running Norton AntiVirus Corporate Edition on ports 1111, 2222, and 3333 (no spaces between port numbers). For example:

```
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.

New Vulnerability Checks

Multiple Buffer Overflows in PHP allow remote access to server

NetRecon can discover network resources running web servers and versions of PHP 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.

Security Update 7

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, obtained from the webserver banner.

Security Update 6

New Objectives

Discover Trojans and vulnerable services running on UDP ports

This objective discovers Trojans and vulnerable services using the UDP protocol by communicating with them on their own ports in addition to determining that the port is open, thus avoiding false positives from benign processes using a port known to be used by some Trojans and vulnerable services.

Discover Trojans and vulnerable services running on TCP ports

This objective discovers Trojans and vulnerable services using the TCP protocol by communicating with them on their own ports in addition to determining that the port is open, thus avoiding false positives from benign processes using a port known to be used by some Trojans and vulnerable services.

New Vulnerability Checks

Universal Plug and Play Service Identified

NetRecon can discover a network resource running the Universal Plug and Play service by communicating with the Universal Plug and Play service to verify its existence. It is strongly recommended to 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.

Security Update 5

New Objectives

Discover trojans running on UDP ports

This objective discovers trojans using the UDP protocol by communicating with them on their own ports in addition to determining that the port is open, thus avoiding false positives from benign processes using a port known to be used by some trojans.

New Vulnerability Checks

Security Update 5 introduces five new vulnerability checks. Versions of these checks already exist in the database, however these checks go one step further in identifying not only the open port, but the particular trojan using the UDP protocol.

mstream trojan horse master allows attack-by-proxy

NetRecon can discover a network resource running a 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

NetRecon can discover a network resource running a 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.

wintrinoo trojan horse daemon allows attack-by-proxy

NetRecon can discover a network resource running a wintrinoo 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 is unlikely to yield a false positive.

trinoo trojan horse daemon allows attack-by-proxy

NetRecon can discover a network resource 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

NetRecon can discover a network resource 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 4

New Features

ESM Integration

The ESM integration has been updated to integrate with ESM 5.5 as part of the SU installation and will be functional for all future SUs.

By default, NetRecon automatically prompts the user to re-register with ESM. Additionally, a shortcut (ESM Registration Tool) will be installed in the NetRecon directory in the start menu

(Start>Programs>Symantec>NetRecon 3.5). If ESM is installed, but not registered with NetRecon, only the shortcut will be installed in the NetRecon directory.

The new ESM Registration Tool launches `esmregister.exe`, allowing the user to register NetRecon with ESM at anytime. The ESM Registration Tool also repairs broken ESM registrations to ESM 5.5. ESM files registered with NetRecon will be updated to SU4.

If an ESM agent is not installed, the NetRecon integration will not be prompted for.

New Objectives

Discover network resources not running Norton AntiVirus Corporate Edition

This objective only reports 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 will only report 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 NetRecon will generate a *service not detected* message.

Security Update 3

New Vulnerability Checks

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

The following is a list of the new web server vulnerability checks.

1. HTTP allows CGI access to .html/...../config.sys
2. HTTP allows CGI access to _vti_bin/shtml.dll
3. HTTP allows CGI access to _vti_inf.html
4. HTTP allows CGI access to _vti_pvt/administrators.pwd
5. HTTP allows CGI access to _vti_pvt/authors.pwd
6. HTTP allows CGI access to _vti_pvt/service.grp
7. HTTP allows CGI access to _vti_pvt/service.pwd
8. HTTP allows CGI access to _vti_pvt/users.pwd
9. HTTP allows CGI access to achg.htr
10. HTTP allows CGI access to aexp.htr
11. HTTP allows CGI access to aexp2.htr
12. HTTP allows CGI access to aexp2b.htr
13. HTTP allows CGI access to aexp3.htr
14. HTTP allows CGI access to aexp4.htr
15. HTTP allows CGI access to aexp4b.htr
16. HTTP allows CGI access to anot.htr
17. HTTP allows CGI access to anot3.htr

18. HTTP allows CGI access to autoexec.bat
19. HTTP allows CGI access to carbo.dll
20. HTTP allows CGI access to config.sys
21. HTTP allows CGI access to doc
22. HTTP allows CGI access to etc/group
23. HTTP allows CGI access to etc/passwd
24. HTTP allows CGI access to iisadmin/bdir.htm
25. HTTP allows CGI access to iisadmin/ism.dll
26. HTTP allows CGI access to passwd
27. HTTP allows CGI access to passwd.pwd
28. HTTP allows CGI access to passwd.pwl
29. HTTP allows CGI access to passwd.txt
30. HTTP allows CGI access to password
31. HTTP allows CGI access to password.pwd
32. HTTP allows CGI access to password.pwl
33. HTTP allows CGI access to password.txt
34. HTTP allows execution of AT-admin.cgi CGI
35. HTTP allows execution of AnyBoard.cgi CGI
36. HTTP allows execution of AnyForm.cgi CGI
37. HTTP allows execution of AnyForm2 CGI
38. HTTP allows execution of CGIemail.exe CGI
39. HTTP allows execution of Count.cgi CGI
40. HTTP allows execution of FormHandler.cgi CGI
41. HTTP allows execution of GetFile.cfm CGI
42. HTTP allows execution of _AuthChangeUrl CGI
43. HTTP allows execution of _vti_bin/shtml.exe CGI

44. HTTP allows execution of _vti_pvt/shtml.exe CGI
45. HTTP allows execution of adminlogin CGI
46. HTTP allows execution of adsamples/config/site.csc CGI
47. HTTP allows execution of aglimpse CGI
48. HTTP allows execution of alibaba.pl | dir CGI
49. HTTP allows execution of args.bat CGI
50. HTTP allows execution of args.cmd CGI
51. HTTP allows execution of ax-admin.cgi CGI
52. HTTP allows execution of ax.cgi CGI
53. HTTP allows execution of bb-hist.sh CGI
54. HTTP allows execution of bigconf.cgi CGI
55. HTTP allows execution of bnbform.cgi CGI
56. HTTP allows execution of catalog_type.asp CGI
57. HTTP allows execution of cgi-shl/win-c-sample.exe CGI
58. HTTP allows execution of cgiwrap CGI
59. HTTP allows execution of classifieds.cgi CGI
60. HTTP allows execution of convert.bas CGI
61. HTTP allows execution of counter.exe CGI
62. HTTP allows execution of day5datacopier.cgi CGI
63. HTTP allows execution of day5datanotifier.cgi CGI
64. HTTP allows execution of default.asp CGI
65. HTTP allows execution of dfire.cgi CGI
66. HTTP allows execution of displayopenedfile.cfm CGI
67. HTTP allows execution of domcfg.nsf CGI
68. HTTP allows execution of dumpenv.pl CGI
69. HTTP allows execution of edit.pl CGI

70. HTTP allows execution of environ.cgi CGI
71. HTTP allows execution of envout.bat CGI
72. HTTP allows execution of exprcalc.cfm CGI
73. HTTP allows execution of faxsurvey CGI
74. HTTP allows execution of filemail.pl CGI
75. HTTP allows execution of files.pl CGI
76. HTTP allows execution of formmail.pl CGI
77. HTTP allows execution of fpcount.exe CGI
78. HTTP allows execution of fpexplore.exe CGI
79. HTTP allows execution of gH.cgi CGI
80. HTTP allows execution of glimpse CGI
81. HTTP allows execution of guestbook.cgi CGI
82. HTTP allows execution of guestbook.pl CGI
83. HTTP allows execution of handler CGI
84. HTTP allows execution of handler.cgi CGI
85. HTTP allows execution of info2www CGI
86. HTTP allows execution of input.bat CGI
87. HTTP allows execution of input2.bat CGI
88. HTTP allows execution of kcms_configure CGI
89. HTTP allows execution of maillist.pl CGI
90. HTTP allows execution of man.sh CGI
91. HTTP allows execution of nph-publish CGI
92. HTTP allows execution of nph-test-cgi CGI
93. HTTP allows execution of openfile.cfm CGI
94. HTTP allows execution of perl/files.pl CGI
95. HTTP allows execution of perlshop.cgi CGI

96. HTTP allows execution of pfdisplay.cgi CGI
97. HTTP allows execution of pfieffer.bat CGI
98. HTTP allows execution of pfieffer.cmd CGI
99. HTTP allows execution of phf.cgi CGI
100. HTTP allows execution of phf.pp CGI
101. HTTP allows execution of php CGI
102. HTTP allows execution of php.cgi CGI
103. HTTP allows execution of ppdscgi.exe CGI
104. HTTP allows execution of queryhit.htm CGI
105. HTTP allows execution of responder.cgi CGI
106. HTTP allows execution of rguest.exe CGI
107. HTTP allows execution of rwwwshell.pl CGI
108. HTTP allows execution of s97.cgi CGI
109. HTTP allows execution of s97r.cgi CGI
110. HTTP allows execution of search.cgi CGI
111. HTTP allows execution of search97.vts CGI
112. HTTP allows execution of sendform.cgi CGI
113. HTTP allows execution of sendmail.cfm CGI
114. HTTP allows execution of showcode.asp CGI
115. HTTP allows execution of startstop.html CGI
116. HTTP allows execution of status.cgi CGI
117. HTTP allows execution of survey.cgi CGI
118. HTTP allows execution of test.bat CGI
119. HTTP allows execution of textcounter.pl CGI
120. HTTP allows execution of tools/getdrvs.exe CGI
121. HTTP allows execution of tools/newdsn.exe CGI

- 122. HTTP allows execution of tst.bat CGI
- 123. HTTP allows execution of unlg1.1 CGI
- 124. HTTP allows execution of unlg1.2 CGI
- 125. HTTP allows execution of upload.pl CGI
- 126. HTTP allows execution of uploader.exe CGI
- 127. HTTP allows execution of view-source CGI
- 128. HTTP allows execution of visadmin.exe CGI
- 129. HTTP allows execution of w3-mysql CGI
- 130. HTTP allows execution of webbbs.cgi CGI
- 131. HTTP allows execution of webdist.cgi CGI
- 132. HTTP allows execution of webgais CGI
- 133. HTTP allows execution of webhits.exe CGI
- 134. HTTP allows execution of websendmail CGI
- 135. HTTP allows execution of webwho.pl CGI
- 136. HTTP allows execution of wguest.exe CGI
- 137. HTTP allows execution of whois_raw.cgi CGI
- 138. HTTP allows execution of wrap CGI
- 139. HTTP allows execution of wrap.cgi CGI
- 140. HTTP allows execution of www-sql CGI
- 141. HTTP allows execution of wwwadmin.pl CGI
- 142. HTTP allows execution of wwwboard.cgi CGI
- 143. HTTP allows execution of wwwboard.pl CGI

Security Update 2

New Vulnerability Checks

Code Red II

NetRecon can discover a Microsoft IIS server that is infected with a variant of the Code Red worm 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

NetRecon can discover a version of Oracle TNS listener 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 allow a remote attacker to 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

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 servers document root. However, because IIS decodes some of the input twice and security checks are only applied 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 will allow the remote intruder to run commands on the IIS server.

Tomcat allows directory traversal

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

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. NetRecon detects both of these exploit methods. Disclosure of this type of information can provide remote intruders with possible vulnerabilities they can exploit.

Security Update 1

New Objectives

IIS Indexing Service exposure may allow remote compromise

This objective discovers 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.