Release Notes

NetRecon™

Version 2.0.2

Security Update

AXENT™

security that means business

The information in this document is subject to change without notice and must not be construed as a commitment on the part of AXENT Technologies. AXENT Technologies 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.

CONTAINS CONFIDENTIAL AND PROPRIETARY INFORMATION OF AXENT TECHNOLOGIES, INC.

Additional copies of this document or of other AXENT Technologies publications may be ordered from your AXENT Account Manager.

For U.S. Technical Support:	**Phone:**	**(801) 227-3700**
	Fax:	**(801) 227-3788**
	E-mail:	**support@axent.com**
For U.K. Technical Support	**Phone:**	**+44 (0) 1372 214321**
	Fax:	**+44 (0) 1372 214341**
	E-mail:	**support@axent.co.uk**
For Licensing Issues:	**Phone:**	**(888) 584-3925**
	Fax:	**(781) 487-9818**
	E-mail:	**license@axent.com**

Trademarks

AXENT Technologies is a registered trademark of AXENT Technologies, Inc.; NetRecon and the AXENT 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: March 1999

Contents

Release Notes

Security Update 2.0.2

NetRecon Security Update 2.0.2 is an add-on for NetRecon 2.0 that increases the number of vulnerabilities NetRecon can check for, changes some objectives, and enhances some existing vulnerability checks. Installing the Security Update adds several new files to the NetRecon 2.0 program directory and modifies several other NetRecon program files. NetRecon Security Update 2.0.2 includes all the vulnerability checks and program enhancements in Security Update 2.0.1 (which at the time of its release was called Vulnerability Pack 1).

Installing

From the Web

If you downloaded the Security Update from the web, the Security Update is a self-extracting executable that, when executed, runs a setup program. To install the Security Update, run the executable (double-click its icon in the Windows Explorer or choose Start, Run, click Browse, locate the Security Update executable, then click Open, then click OK). Follow the prompts in the setup program.

The setup program automatically finds the location of the NetRecon 2.0 folder on your hard disk and modifies and adds the appropriate files in that folder.

From a CD

If you received the Security Update on a CD, you simply need to insert the CD to launch the NetRecon Installation Menu. Click Install, then click Install Security Update 2.0.2 and follow the setup program instructions.

The setup program automatically finds the location of the NetRecon 2.0 folder on your hard disk and modifies and adds the appropriate files in that folder.

Enhancements

Registry Checks

NetRecon now includes a module for checking Windows registry keys and values, greatly improving its ability to assess the security of Windows network resources. A large number of registry-related vulnerability checks have been added using this module.

Improved ICMP Module

The module for detecting network resources using the ICMP protocol (ping being one example) has been enhanced and expanded. NetRecon now tries to detect a system numerous times using ICMP, in case any packets are dropped. NetRecon also performs a wider range of ICMP requests, making it more likely to detect network resources through firewalls. Several new vulnerability checks have been added using this enhanced module.

Improved NetWare Checks

NetRecon now includes a file analysis module that can check for the presence or absence of certain files, configuration data within files, and so forth. This module can sometimes read the Service Advertising Protocol (SAP) broadcast tables stored on NetWare servers. Novell NetWare devices use SAP to "advertise" their names, addresses and current state to the network. For example, NetRecon uses this protocol to determine which NetWare systems are running rconsole, which is known to have vulnerabilities.

Reduced False Positives

NetRecon now includes improved analysis of some systems and services that reduces the number of false positives that can be reported.

New Vulnerability Checks

Security Update 2.0.2 includes 75 new vulnerability checks. The majority of the new vulnerability checks in 2.0.2 are Windows registry checks, made possible by the new registry analysis module. Security Update 2.0.2 also includes several new ICMP checks.

Examples of New Vulnerability Checks

Following are some examples of checks added:

Run key has vulnerable permissions

NetRecon has discovered that permissions on the Run registry key do not conform to Microsoft’s recommended security settings. The Run key contains a list of applications to be run when Windows starts. An attacker with permission to modify this key could specify a trojan horse application to run or a malicious use of an existing program on the target system or network. An attacker could also potentially disable security software that should be run on startup (such as a virus checker).

LanManager authentication permitted

NetRecon has discovered a Windows system that permits LanManager authentication, which uses a weaker form of encryption than Windows NT authentication. Many systems permit this by default for compatibility with Windows 95 and NetWare clients. An attacker could potentially sniff and then crack the LanManager password hash.

responds to ICMP information request

NetRecon has discovered that this system responds to an ICMP information request. ICMP is part of the IP layer. It is used to handle IP status and control messages. The ICMP information request message type is an obsolete ICMP message request; however, some systems still respond to it.

The following are known threats to the use of this protocol:

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information "under the noses" of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o’ Death attack. The Ping o’ Death attack sends an oversized ping packet in an attempt to overflow the system’s buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Complete List of New Vulnerability Checks

Following is the complete list of vulnerability checks added in Security Update 2.0.2:

ICMP Checks
network resource detected via ICMP protocol
network detected via ICMP protocol
responds to ICMP information request
responds to UDP requests with ICMP
responds to ICMP timestamp request
responds to ICMP echo request (ping)
responds to ICMP address mask request

Miscellaneous Checks
Sendmail daemon mode bug allows shell users root access

NetWare Checks
rconsole service enabled

Registry Checks
.Default key has vulnerable permissions
AeDebug key has vulnerable permissions
AppId key has vulnerable permissions
auditing of rights not enabled
autologin feature enabled
base system objects not sufficiently protected
base system objects not audited
Compatibility key has vulnerable permissions
CurrentVersion key has vulnerable permissions
DCOM enabled
default password in plain text in registry
Drivers key has vulnerable permissions
Embedding key has vulnerable permissions
event auditing failure permitted
Font Drivers key has vulnerable permissions
FontCache key has vulnerable permissions
FontMapper key has vulnerable permissions

Fonts key has vulnerable permissions
FontSubstitutes key has vulnerable permissions
GRE_Initialize key has vulnerable permissions
guest account can access security event log
guest account can access system event log
guest account can access application event log
HKEY_LOCAL_MACHINE hive has vulnerable permissions
Internet Explorer 3.0 or 3.01 found
Internet Explorer 4.x missing Service Pack 1
Internet Explorer 3.02 missing Year 2000 patch
Internet Explorer 4.0 missing Dotless IP patch
Internet Explorer 4.0 missing Untrusted Script Paste patch
LanManager authentication permitted
legal notice logon banner not enabled
local users can install print drivers
logon dialog box allows system shutdown
MCI Extensions key has vulnerable permissions
MCI key has vulnerable permissions
named pipes RPC denial of service possible
network access to floppy disk drive possible
network access to CD-ROM possible
non-administrator job scheduling permitted
non-administrator remote registry access possible
Ole key has vulnerable permissions
OS/2 subsystem enabled
password filter not enabled
PerfLib key has vulnerable permissions
Port key has vulnerable permissions
POSIX subsystem enabled
ProfileList key has vulnerable permissions
Regfile shell open command key has vulnerable permissions
registry files associated with regedit.exe
RPC key has vulnerable permissions
Run key has vulnerable permissions
RunOnce key has vulnerable permissions
Shares key has vulnerable permissions
SMB message signing disabled (client)
SMB message signing disabled (server)
Software hive has vulnerable permissions

Type 1 Installer key has vulnerable permissions
Uninstall key has vulnerable permissions
unrestricted null session enumeration possible
UPS key has vulnerable permissions
username of last login displayed
ValidCommunities key has vulnerable permissions
Windows NT page file not cleared at system shutdown
Windows NT system caches logon credentials
Windows3.1MigrationStatus key has vulnerable permissions
Winlogon key has vulnerable permissions
WOW key has vulnerable permissions

Changed Objectives

The **Extract information from icmp packets** and **Discover network resources that respond to ping** objectives have now been combined into the **Use ICMP protocol to scan network resources** objective.

Known Issues

There are a number of vulnerabilities added in this security update that check for proper permissions on registry keys (they all have a vulnerability name **[key name] key has vulnerable permissions**). In those cases, the solution suggested (in the vulnerability documentation, which can be shown by choosing Report, View Vulnerability Descriptions, or by clicking a vulnerability name in a report to see its description) lists the permissions Microsoft recommends. That list constitutes *all* the permissions that should be allowed. If users or groups not on that list have been given any type of permission, NetRecon will report that condition as a vulnerability.

Security Update 2.0.1

Enhancements

Reduced False Positives

Whenever NetRecon can access the registry on a Windows system, it can now check for the presence of Windows HotFixes. Since some vulnerabilities (denial of service vulnerabilities, for example) are reported based on version information, NetRecon would sometimes report false positives and recommend installing a HotFix that had already been installed. Being able to detect Windows HotFixes eliminates some false positives.

More Services and Operating Systems Identified

Existing vulnerability checks that identify services and operating systems can now succcessfully identify a wider range of such products.

New Vulnerability Checks

Following is a complete list of vulnerability checks added in Security Update 2.0.1:

FTP Checks
anonymous FTP access is enabled
FTP access obtained
FTP root directory is writable
ftpd backdoor allows anonymous users root access

Firewall Checks
identified firewall

NetWare File Analysis Checks
NetWare console not secured
NetWare rconsole password obtained from AUTOEXEC.NCF

NetWare server with DOS not removed from memory
NetWare startup file read access obtained
NetWare startup file write access obtained
NetWare telnet server allows insecure remote console access

Miscellaneous Checks
administrative shell access obtained via site exec
IRC server identified
NetBus backdoor service identified
nfs service enabled
SLmail paren denial of service
SLmailNT paren denial of service
ssh service enabled
teardrop attack (IP fragmentation overlap) possible
tetrinet service enabled
user shell access obtained via site exec

New Objectives

The following objectives were added in Security Update 2.0.1:

Discover Finger vulnerabilities

This objective probes identified finger servers for configuration errors and other finger-related security problems.

Discover FTP vulnerabilities

This objective probes identified FTP servers for common configuration problems, known security-related bugs, and back doors.

Discover IRC vulnerabilities

This objective attempts to identify IRC servers and associated security problems.

Discover vulnerabilities by analyzing files

This objective examines the contents of file systems accessed by NetRecon, searching for certain key files whose absence, presence, attributes, or contents constitute vulnerabilities.

For example, if NetRecon can find and read NetWare system configuration files (such as `autoexec.ncf`), which may be a vulnerability in and of itself, it searches for misconfigurations within these files, tries to determine whether they have correctly assigned file attributes, and so forth.