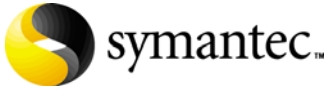
Symantec ESM 6.5 Network Assessment Security Update 31.07 Release Notes



Symantec ESM 6.5 Network Assessment Security Updates Release Notes

Technical support

As part of Symantec Security Response, the Symantec Global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site at http://www.symantec.com/techsupp/ for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Platinum Technical Support customers have access to the PlatinumWeb site: https://www-secure.symantec.com/platinum/login.html.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
Symantec Enterprise Security Manager

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "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 AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use that number of copies of the Software as have been licensed to You by Symantec under a License Module. Permission to use the software to assess Desktop, Server or Network machines does not constitute permission to make additional copies of the Software. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software you are authorized to use on a single machine.
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software to assess no more than the number of Desktop machines set forth under a License Module. "Desktop" means a desktop central processing unit for a single end user;
D. use the Software to assess no more than the number of Server machines set forth under a License Module. "Server" means a central processing unit that acts as a server for other central processing units;
E. use the Software to assess no more than the number of Network machines set forth under a License Module. "Network" means a system comprised of multiple machines, each of which can be assessed over the same network;
F. use the Software in accordance with any written agreement between You and Symantec; and
G. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;
B. use the Software to assess a Desktop, Server or Network machine for which You have not been granted permission under a License Module;
C. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
D. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
E. continue to use a previously issued license key if You have received a new license key for such license, such as with a disk replacement set or an upgraded version of the Software, or in any other instance;
F. continue to use a previous version or copy of the Software after You have installed a disk replacement set, an upgraded version, or other authorized replacement. Upon such replacement, all copies of the prior version must be destroyed;
G. use a later version of the Software than is provided herewith unless you have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
H. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module; nor
I. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following

Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of the Software to any entity not authorized by, or that is specified by, the United States Federal Government is strictly prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the

laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software 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 communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Security Update Release Notes

Security Update Release Notes

September 21, 2007 (Security Update 31.07)

This content update for Symantec ESM Network Assessment detects and reports one additional vulnerability.

The following table includes information about the additional vulnerability.

Bugtraq ID	Vulnerability Name
25566	MS agentdpv.dll ActiveX Control Malformed URL Stack Buffer Overflow Vulnerability

August 30, 2007 (Security Update 31.06)

This content update for Symantec ESM Network Assessment detects and reports 5 additional vulnerabilities. The following table includes information about the additional vulnerabilities.

Bugtraq ID	Vulnerability Name
25282	Microsoft OLE Automation SubstringData Function Integer Overflow Vulnerability
25289	Microsoft Visual Basic 6 TBLinf32.DLL ActiveX Control Remote Code Execution Vulnerability
25295	MS Visual Basic 6 Package and Deployment Wizard ActiveX Control Remote Code Execution Vulnerability
25302	Microsoft Windows GDI Metafiles AttemptWrite Remote Code Execution Vulnerability

Bugtraq ID	Vulnerability Name
25310	Microsoft Internet Explorer Vector Markup Language VGX.DLL Remote Buffer Overflow Vulnerability

July 26, 2007 (Security Update 31.04)

This content update for Symantec ESM Network Assessment detects and reports 3 additional vulnerabilities. The following table includes information about the additional vulnerabilities.

Bugtraq ID	Vulnerability Name
24796	Microsoft Windows Active Directory LDAP Request Validation Remote Denial Of Service Vulnerability
24800	Microsoft Windows Active Directory LDAP Request Validation Remote Code Execution Vulnerability
15921	Microsoft Internet Information Server 5.1 DLL Request Remote Code Execution Vulnerability

June 22, 2007 (Security Update 30.04)

This content update for Symantec ESM Network Assessment detects and reports 12 additional vulnerabilities. The following table includes information about the additional vulnerabilities.

Bugtraq ID	Vulnerability Name
24416	Microsoft Windows SChannel Security Remote Code Execution Vulnerability
17717	Outlook Express/Windows Mail MHTML URI Handler Information Disclosure Vulnerability
24392	Microsoft Outlook Express MHTML URL Parsing Information Disclosure Vulnerability
24410	Microsoft Outlook Express Content Disposition Parsing Information Disclosure Vulnerability
24370	Microsoft Win32 API Parameter Validation Remote Code Execution Vulnerability
24372	Microsoft Internet Explorer URLMON.DLL COM Object Instantiation Remote Code Execution Vulnerability

Bugtraq ID	Vulnerability Name
24418	Microsoft Internet Explorer Prototype Variable Uninitialized Memory Corruption Vulnerability
24426	Microsoft Internet Explorer Speech API 4 COM Object Instantiation Buffer Overflow Vulnerabilities
24429	Microsoft Internet Explorer Language Pack Installation Remote Code Execution Vulnerability
24423	Microsoft Internet Explorer CSS Tag Memory Corruption Vulnerability
22966	Microsoft Internet Explorer NavCancel.HTM Cross-Site Scripting Vulnerability
24448	RETIRED: Microsoft Internet Explorer Navigation Cancel Webpage Spoofing Vulnerability

Known Issue

The following issue is known in the Symantec ESM Network Assessment June 22, 2007 release:

- The vulnerabilities for Internet Explorer 7 on Windows Server 2003 are not reported.

May 21, 2007 (Security Update 30.02)

This content update for Symantec ESM Network Assessment detects and reports 12 additional vulnerabilities. The following table includes information about the additional vulnerabilities.

Bugtraq ID	Vulnerability Name
23470	Microsoft Windows DNS Server Escaped Zone Name Parameter Buffer Overflow Vulnerability
19529	Microsoft Internet Explorer CHTSKDIC.DLL Arbitrary Code Execution Vulnerability
21207	Acer LunchApp.APlunch ActiveX Control Remote Code Execution Vulnerability
23331	Research In Motion Blackberry TeamOn Import Object ActiveX Control Buffer Overflow Vulnerability
23769	Microsoft Internet Explorer Property Method Remote Code Execution Vulnerability

Bugtraq ID	Vulnerability Name
23770	Microsoft Internet Explorer HTML Objects Script Errors Variant Remote Code Execution Vulnerability
23771	Microsoft Internet Explorer Object Handling Remote Code Execution Vulnerability
23772	Microsoft Internet Explorer HTML Objects Script Errors Remote Code Execution Vulnerability
23806	Microsoft Outlook Web Access Remote Script Injection Vulnerability
23808	Microsoft Exchange iCal Request Remote Denial of Service Vulnerability
23809	Microsoft Exchange Base64 MIME Message Remote Code Execution Vulnerability
23810	Microsoft Exchange IMAP Command Processing Remote Denial of Service Vulnerability

April 20, 2007 (Security Update 30.01)

This content update for Symantec ESM Network Assessment detects and reports 13 additional vulnerabilities. The following table includes information about the additional vulnerabilities.

Bugtraq ID	Vulnerability Name
20940	Microsoft Windows GDI Kernel Local Privilege Escalation Vulnerability
23194	Microsoft Windows Cursor And Icon ANI Format Handling Remote Buffer Overflow Vulnerability
23273	Microsoft Windows Graphics Rendering Engine GDI Local Privilege Escalation Vulnerability
23275	Microsoft Windows GDI WMF Remote Denial of Service Vulnerability
23276	Microsoft Windows Graphics Device Interface Font Rasterizer Local Privilege Escalation Vulnerability
23277	Microsoft Windows GDI Invalid Window Size Local Privilege Escalation Vulnerability
23278	Microsoft Windows Graphics Rendering Engine EMF File Privilege Escalation Vulnerability
11694	LibXPM Multiple Unspecified Vulnerabilities

Bugtraq ID	Vulnerability Name
23371	Microsoft Windows UPnP Remote Stack Buffer Overflow Vulnerability
23337	Microsoft Agent URI Processing Remote Code Execution Vulnerability
21688	Microsoft Windows CSRSS HardError Messages Denial of Service Vulnerability
23324	Microsoft Windows CSRSS MSGBox Remote Code Execution Vulnerability
23367	Windows VDM Zero Page Race Condition Local Privilege Escalation Vulnerability

February 21, 2007 (Security Update 29.02)

This content update for Symantec ESM Network Assessment detects and reports 9 additional vulnerabilities. The following table includes information about the additional vulnerabilities.

Bugtraq ID	Vulnerability Name
22478	Microsoft HTML Help ActiveX Control Remote Code Execution Vulnerability
20704	Microsoft Internet Explorer ADODB.Connection Execute Memory Corruption Vulnerability
22486	Microsoft Internet Explorer IM JPCKSI COM Object Instantiation Memory Corruption Vulnerability
22489	Microsoft Internet Explorer WinINet.DLL FTP Server Response Parsing Memory Corruption Vulnerability
22504	Microsoft Internet Explorer COM Object Instantiation Variant Memory Corruption Vulnerability
22481	Microsoft Windows Shell Hardware Detection Service Privilege Escalation Vulnerability
22499	Microsoft Windows Image Acquisition Service Privilege Escalation Vulnerability
22483	Microsoft Windows OLE Dialog Remote Code Execution Vulnerability
22476	Microsoft MFC Embedded OLE Object Remote Code Execution Vulnerability

January 22, 2007 (Security Update 29.01)

This content update for Symantec ESM Network Assessment detects and reports 1 additional vulnerability. The following table includes information about the additional vulnerability.

Bugtraq ID	Vulnerability Name
21930	Microsoft Windows Vector Markup Language Buffer Overrun Vulnerability

December 20, 2006 (Security Update 28.03)

This content update for Symantec ESM Network Assessment detects and reports 10 additional vulnerabilities. The following table includes information about the 10 additional vulnerabilities.

Bugtraq ID	Vulnerability Name
21552	Microsoft Internet Explorer Script Error Handling Remote Code Execution Vulnerability
21507	Microsoft Internet Explorer Object Tag TIF Folder Information Disclosure Vulnerability
21494	Microsoft Internet Explorer Drag and Drop TIF Folder Information Disclosure Vulnerability
21546	Microsoft Internet Explorer DHTML Script Function Remote Code Execution Vulnerability
21505	Windows Media Player Remote ASF File Buffer Overflow Vulnerability
21247	Windows Media Player ASX PlayList File Heap Overflow Vulnerability
21537	Microsoft Windows SNMP Service Remote Code Execution Vulnerability
21550	Microsoft Windows Manifest File Privilege Escalation Vulnerability
21501	Microsoft Outlook Express Windows Address Book Contact Record Remote Code Execution Vulnerability
21495	Microsoft Windows 2000 Remote Installation Service Remote Code Execution Vulnerability

November 20, 2006 (Security Update 28.02)

This content update for Symantec ESM Network Assessment detects and reports 9 additional vulnerabilities. The following table includes information about the 9 additional vulnerabilities.

Bugtraq ID	Vulnerability Name
19738	Microsoft Internet Explorer Daxctle.OCX Spline Method Heap Buffer Overflow Vulnerability
20047	Microsoft Internet Explorer Daxctle.OCX KeyFrame Method Heap Buffer Overflow Vulnerability
21020	Microsoft Internet Explorer HTML Rendering Remote Code Execution Vulnerability
21034	Microsoft Agent ActiveX Control Remote Code Execution Vulnerability
20985	Microsoft Windows Workstation Service NetpManageIPCConnect Remote Code Execution Vulnerability
20984	Microsoft Client Service for Netware Denial of Service Vulnerability
21023	Microsoft Windows Client Service For Netware Remote Code Execution Vulnerability
19980	Adobe Flash Player Multiple Remote Code Execution Vulnerabilities
18894	Macromedia Flash Malformed SWF File Multiple Vulnerabilities

October 31, 2006 (Security Update 28.01)

This content update for Symantec ESM Network Assessment detects and reports 10 additional vulnerabilities. The following table includes information about the 10 additional vulnerabilities.

Bugtraq ID	Vulnerability Name
20096	Microsoft Internet Explorer Vector Markup Language Buffer Overflow Vulnerability
19030	Microsoft WebViewFolderIcon ActiveX Control Buffer Overflow Vulnerability
20338	Microsoft Windows XML Core Services XSLT Buffer Overrun Vulnerability
20339	Microsoft XML Core Services Information Disclosure Vulnerability

Bugtraq ID	Vulnerability Name
19215	Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability
20373	Microsoft Windows SMB Rename Remote Denial of Service Vulnerability
10183	Multiple Vendor TCP Sequence Number Approximation Vulnerability
13124	Multiple Vendor TCP/IP Implementation ICMP Remote Denial Of Service Vulnerabilities
13658	Microsoft IPv6 TCP/IP Loopback LAND Denial of Service Vulnerability
20318	Microsoft Windows Object Packager Remote Code Execution Vulnerability

September 26, 2006 (Security Update 27.03)

This content update for Symantec ESM Network Assessment detects and reports 2 additional vulnerabilities. The following table includes information about the 2 additional vulnerabilities.

Bugtraq ID	Vulnerability Name
19922	Microsoft PGM Remote Buffer Overflow Vulnerability
19927	Microsoft Indexing Service Query Validation Cross-Site Scripting Vulnerability

August 21, 2006 (Security Update 27.02)

This content update for Symantec ESM Network Assessment detects and reports 44 additional vulnerabilities and 67 updated vulnerabilities. The following table includes information about the 44 additional vulnerabilities.

Bugtraq ID	Vulnerability Name
11826	Microsoft Internet Explorer FTP URI Arbitrary FTP Server Command Execution Vulnerability
18198	Microsoft Windows MHTML URI Buffer Overflow Vulnerability
18277	Microsoft Internet Explorer Frameset Memory Corruption Vulnerability
18500	Microsoft HLINK.DLL Link Memory Corruption Vulnerability
18682	Microsoft Internet Explorer OuterHTML Redirection Handling Information Disclosure Vulnerability

Bugtraq ID	Vulnerability Name
18769	Microsoft Windows HTML Help HHCtrl ActiveX Control Memory Corruption Vulnerability
18855	Microsoft Internet Explorer Structured Graphics Control Denial Of Service Vulnerability
18873	Microsoft Internet Explorer Table Frameset Denial Of Service Vulnerability
18900	Microsoft Internet Explorer 6 RDS.DataControl Denial Of Service Vulnerability
18902	Microsoft Internet Explorer DirectAnimation.DAUserData Denial Of Service Vulnerability
18903	Microsoft Internet Explorer Object.Microsoft.DXTFilter Denial Of Service Vulnerability
18929	Microsoft Internet Explorer HtmlDlgSafeHelper Remote Denial Of Service Vulnerability
18946	Microsoft Internet Explorer TriEditDocument Denial Of Service Vulnerability
18960	Microsoft Internet Explorer RevealTrans Denial Of Service Vulnerability
19030	Microsoft Internet Explorer WebViewFolderIcon Denial Of Service Vulnerability
19069	Microsoft Internet Explorer DataSourceControl Denial of Service Vulnerability
19079	Microsoft Internet Explorer OVCtl Denial Of Service Vulnerability
19092	Microsoft Internet Explorer Content-Type Denial Of Service Vulnerability
19102	Microsoft Internet Explorer String To Binary Function Denial Of Service Vulnerability
19109	Microsoft Internet Explorer Internet.HHCtrl Click Denial Of Service Vulnerability
19113	Microsoft Internet Explorer Multiple Object ListWidth Property Denial Of Service Vulnerability
19114	Microsoft Internet Explorer NMSA.ASFSourceMediaDescription Stack Overflow Vulnerability
19135	Microsoft Windows Remote Denial of Service Vulnerability

Bugtraq ID	Vulnerability Name
19140	Microsoft Internet Explorer Native Function Iterator Denial Of Service Vulnerability
19184	Microsoft Internet Explorer NDFXArtEffects Stack Overflow Vulnerability
19215	Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability
19221	Microsoft Windows Graphical Device Interface Plus Library Denial Of Service Vulnerability
19227	Microsoft Internet Explorer ADODB.Recordset NextRecordset Denial of Service Vulnerability
19228	Microsoft Internet Explorer Deleted Frame Object Denial Of Service Vulnerability
19300	Microsoft Windows Routing and Remote Access Denial of Service Vulnerability
19312	Microsoft Internet Explorer HTML Layout and Positioning Remote Code Execution Vulnerability
19316	Microsoft Internet Explorer Chained Cascading Style Sheets Remote Code Execution Vulnerability
19319	Microsoft Winsock Gethostbyname Buffer Overflow Vulnerability
19339	Microsoft Internet Explorer Window Location Cross-Domain Information Disclosure Vulnerability
19340	Microsoft Internet Explorer COM Object Instantiation Code Execution Vulnerability
19375	Microsoft Windows User Profile Privilege Escalation Vulnerability
19384	Microsoft Windows Unhandled Exception Remote Code Execution Vulnerability
19388	Microsoft Windows 2000 Kernel Local Privilege Escalation Vulnerability
19389	Microsoft Windows Explorer Drag and Drop Remote Code Execution Vulnerability
19400	Microsoft Internet Explorer Source Element Cross-Domain Information Disclosure Vulnerability
19404	Microsoft Windows DNS Client Buffer Overrun Vulnerability
19405	Microsoft Hyperlink Object Library Function Remote Buffer Overflow Vulnerability

Bugtraq ID	Vulnerability Name
19409	Microsoft Windows Server Service Remote Buffer Overflow Vulnerability
19417	Microsoft Management Console Zone Bypass Vulnerability

The following table includes information about the 67 updated vulnerabilities.

Bugtraq ID	Vulnerability Name
2206	PHP .htaccess Attribute Transfer Vulnerability
6557	PHP 4.0.3 IMAP Module Buffer Overflow Vulnerability
16220	PHP 5 User-Supplied Session ID Input Validation Vulnerability
15177	PHP Apache 2 Local Denial of Service Vulnerability
15413	PHP Apache 2 Virtual() Safe_Mode and Open_Basedir Restriction Bypass Vulnerability
7256	PHP array_pad() Integer Overflow Memory Corruption Vulnerability
6875	PHP CGI SAPI Code Execution Vulnerability
15411	PHP cURL and GD Multiple Safe_Mode and Open_Basedir Restriction Bypass Vulnerabilities
11557	PHP cURL Open_Basedir Restriction Bypass Vulnerability
8405	PHP DLOpen Memory Disclosure Vulnerability
7199	PHP emalloc() Unspecified Integer Overflow Memory Corruption Vulnerability
2205	PHP Engine Disable Source Viewing Vulnerability
1786	PHP Error Logging Format String Vulnerability
15250	PHP File Upload GLOBAL Variable Overwrite Vulnerability
5681	PHP Function CRLF Injection Vulnerability
12701	PHP Glob Function Local Information Disclosure Vulnerability
13164	PHP Group Exif Module IFD Nesting Denial Of Service Vulnerability
13163	PHP Group Exif Module IFD Tag Integer Overflow Vulnerability
15358	PHP Group Exif Module Infinite Recursion Denial Of Service Vulnerability
12962	PHP Group PHP Image File Format Remote Denial Of Service Vulnerability

Bugtraq ID	Vulnerability Name
13143	PHP Group PHP Multiple Unspecified Vulnerabilities
12963	PHP Group PHP Remote JPEG File Format Remote Denial Of Service Vulnerability
5669	PHP Header Function Script Injection Vulnerability
5278	PHP HTTP POST Incorrect MIME Header Parsing Vulnerability
4063	PHP Include File Relative Directory Information Disclosure Vulnerability
10427	PHP Input/Ouput Wrapper Remote Include Function Command Execution Weakness
5280	PHP Interpreter Direct Invocation Denial Of Service Vulnerability
11992	PHP JPEG Image Buffer Overflow Vulnerability
5562	PHP Mail Function ASCII Control Character Header Spoofing Vulnerability
15571	PHP MB_Send_Mail TO Argument Header Injection Vulnerability
10725	PHP memory_limit Remote Code Execution Vulnerability
10471	PHP Microsoft Windows Shell Escape Functions Command Execution Vulnerability
4325	PHP Move_Uploaded_File Open_Basedir Circumvention Vulnerability
11964	PHP Multiple Local And Remote Vulnerabilities
11981	PHP Multiple Remote Vulnerabilities
4026	PHP MySQL Safe_Mode Filesystem Circumvention Vulnerability
16145	PHP MySQL_Connect Remote Buffer Overflow Vulnerability
16219	PHP MySQLI Error Logging Remote Format String Vulnerability
17688	PHP MySQLI Error Logging Remote Format String Vulnerability_copy
14957	PHP Open_BaseDir Security Restriction Bypass Vulnerability
7210	PHP openlog() Buffer Overflow Vulnerability
15249	PHP Parse_Str Register_Globals Activation Weakness
11334	PHP PHP_Variables Remote Memory Disclosure Vulnerability
7805	PHP PHPInfo Cross-Site Scripting Vulnerability
15248	PHP PHPInfo Cross-Site Scripting Vulnerability

Bugtraq ID	Vulnerability Name
15248	PHP PHPInfo Cross-Site Scripting Vulnerability
4606	PHP posix_getpwnam / posix_getpwuid safe_mode Circumvention Vulnerability
4183	PHP Post File Upload Buffer Overflow Vulnerabilities
11190	PHP Remote Arbitrary Location File Upload Vulnerability
15119	PHP Safedir Restriction Bypass Vulnerabilities
2954	PHP SafeMode Arbitrary File Execution Vulnerability
14858	PHP Session Handling Local Session Hijacking Vulnerability
12045	PHP Shared Memory Module Offset Memory Corruption Vulnerability
7187	PHP socket_iovec_alloc() Integer Overflow Vulnerability
7197	PHP socket_recv() Signed Integer Memory Corruption Vulnerability
7198	PHP socket_recvfrom() Signed Integer Memory Corruption Vulnerability
7259	PHP STR_Repeat Boundary Condition Error Vulnerability
10724	PHP Strip_Tags() Function Bypass Vulnerability
7761	PHP Transparent Session ID Cross Site Scripting Vulnerability
8201	PHP Undefined Safe_Mode_Include_Dir Safemode Bypass Vulnerability
6488	PHP wordwrap() Heap Corruption Vulnerability
911	PHP3 'safe_mode' Failure Vulnerability
8693	PHP4 Base64_Encode() Integer Overflow Vulnerability
8696	PHP4 Multiple Vulnerabilities
12665	PHP4 Readfile Denial Of Service Vulnerability
3873	PHP4 Session Files Local Information Disclosure Vulnerability
14088	XML-RPC for PHP Remote Code Injection Vulnerability

July 21, 2006 (Security Update 27.01)

This content update for Symantec ESM Network Assessment detects and reports 24 additional vulnerabilities and 126 updated vulnerabilities. The following table includes information about the 24 new vulnerabilities.

Bugtraq ID	Vulnerability Name
7539	Internet Explorer file:// Request Zone Bypass Vulnerability
18858	Microsoft IIS ASP Remote Code Execution Vulnerability
3116	Microsoft Internet Explorer Arbitrary HTML File Execution Vulnerability
6779	Microsoft Internet Explorer Dialog Box Cross-Domain Violation Vulnerability
17468	Microsoft Internet Explorer HTML Tag Memory Corruption Vulnerability
6205	Microsoft Internet Explorer IFRAME dialogArguments Cross-Zone Access Vulnerability
11515	Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability
5196	Microsoft Internet Explorer OBJECT Tag Same Origin Policy Violation Vulnerability
7419	Microsoft Internet Explorer Remote URLMON.DLL Buffer Overflow Vulnerability
6780	Microsoft Internet Explorer ShowHelp Arbitrary Command Execution Vulnerability
5963	Microsoft Internet Explorer Unauthorized Document Object Model Access Vulnerability
18923	Microsoft Windows DHCP Client Service Remote Code Execution Vulnerability
18863	Microsoft Windows Server Driver Mailslot Remote Heap Buffer Overflow Vulnerability
18891	Microsoft Windows Server Driver Remote Information Disclosure Vulnerability
9320	Microsoft Windows showHelp CHM File Execution Weakness
14480	Microsoft Windows Unspecified Remote Arbitrary Code Execution Vulnerability

Bugtraq ID	Vulnerability Name
18116	PHP cURL Encoded NULL Character Safe_Mode Restriction Bypass Vulnerability
16803	PHP Error Message Cross-Site Scripting Vulnerability
18645	PHP Error_Log Safe_Mode Restriction-Bypass Vulnerability
17296	PHP Html_Entity_Decode() Information Disclosure Vulnerability
17439	PHP Multiple Safe_Mode and Open_Basedir Restriction Bypass Vulnerabilities
16878	PHP Multiple Security Bypass Vulnerabilities
17843	PHP Multiple Unspecified Vulnerabilities
17362	PHP PHPInfo Large Input Cross-Site Scripting Vulnerability

The following table includes information about the 126 updated vulnerabilities.

Bugtraq ID	Vulnerability Name
10118	Microsoft ASN.1 Library Double Free Memory Corruption Vulnerability
17453	Microsoft Internet Explorer COM Object Instantiation Code Execution Vulnerability
17196	Microsoft Internet Explorer CreateTextRange Remote Code Execution Vulnerability
5561	Microsoft Internet Explorer Dialog Same Origin Policy Bypass Variant Vulnerability
17454	Microsoft Internet Explorer Double Byte Character Memory Corruption Vulnerability
5559	Microsoft Internet Explorer Download Dialogue File Source Obfuscation Vulnerability
17455	Microsoft Internet Explorer Erroneous IOleClientSite Data Zone Bypass Vulnerability
5610	Microsoft Internet Explorer HTML Same Origin Policy Violation Vulnerability
5672	Microsoft Internet Explorer IFrame/Frame Cross-Site/Zone Script Execution Vulnerability
17450	Microsoft Internet Explorer Invalid HTML Parsing Code Execution Vulnerability

Bugtraq ID	Vulnerability Name
14087	Microsoft Internet Explorer Javaprxy.DLL COM Object Instantiation Heap Overflow Vulnerability
5558	Microsoft Internet Explorer Legacy Text Formatting ActiveX Component Buffer Overflow Vulnerability
6217	Microsoft Internet Explorer Object Tag Temporary Internet File Folder Vulnerability
17460	Microsoft Internet Explorer Persistent Window Content Address Bar Spoofing Vulnerability
6216	Microsoft Internet Explorer PNG Buffer Overflow Vulnerability
6366	Microsoft Internet Explorer PNG Deflate Heap Corruption Vulnerability
17457	Microsoft Internet Explorer Popup Cross-Domain Information Disclosure Vulnerability
17131	Microsoft Internet Explorer Script Action Handler Buffer Overflow Vulnerability
17181	Microsoft Internet Explorer Unspecified Remote HTA Execution Vulnerability
5560	Microsoft Internet Explorer XML Redirect File Disclosure Vulnerability
10112	Microsoft Jet Database Engine Remote Code Execution Vulnerability
10113	Microsoft Negotiate SSP Remote Buffer Overflow Vulnerability
8458	Microsoft RPCSS DCERPC DCOM Object Activation Packet Length Heap Corruption Vulnerability
8459	Microsoft RPCSS DCOM Interface Long Filename Heap Corruption Vulnerability
10117	Microsoft Virtual DOS Machine Local Privilege Escalation Vulnerability
11378	Microsoft Window Management API Local Privilege Escalation Vulnerability
10114	Microsoft Windows 2000 Domain Controller LDAP Denial Of Service Vulnerability
2988	Microsoft Windows 2000 SMTP Improper Authentication Vulnerability
10123	Microsoft Windows COM Internet Service/RPC Over HTTP Remote Denial Of Service Vulnerability
8205	Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability

Bugtraq ID	Vulnerability Name
15064	Microsoft Windows Explorer Web View Script Injection Vulnerability
10111	Microsoft Windows H.323 Remote Buffer Overflow Vulnerability
10119	Microsoft Windows Help And Support Center URI Validation Code Execution Vulnerability
11365	Microsoft Windows Kernel Local Denial of Service Vulnerability
11369	Microsoft Windows Kernel Virtual DOS Machine Privilege Escalation Vulnerability
12481	Microsoft Windows License Logging Service Buffer Overflow Vulnerability
10122	Microsoft Windows Local Descriptor Table Local Privilege Escalation Vulnerability
10126	Microsoft Windows Logon Process Remote Buffer Overflow Vulnerability
10108	Microsoft Windows LSASS Buffer Overrun Vulnerability
15070	Microsoft Windows Malicious Shortcut Handling Remote Code Execution Variant Vulnerability
15069	Microsoft Windows Malicious Shortcut Handling Remote Code Execution Vulnerability
10121	Microsoft Windows Object Identity Network Communication Vulnerability
10116	Microsoft Windows Private Communications Transport Protocol Buffer Overrun Vulnerability
8234	Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability
8811	Microsoft Windows RPCSS Multi-thread Race Condition Vulnerability
10127	Microsoft Windows RPCSS Service Remote Denial Of Service Vulnerability
7146	Microsoft Windows Script Engine JScript.DLL Heap Overflow Vulnerability
9510	Microsoft Windows Shell CLSID File Extension Misrepresentation Vulnerability
10115	Microsoft Windows SSL Library Denial of Service Vulnerability
10708	Microsoft Windows Task Scheduler Remote Buffer Overflow Vulnerability

Bugtraq ID	Vulnerability Name
10124	Microsoft Windows Utility Manager Local Privilege Escalation Vulnerability
11763	Microsoft Windows WINS Association Context Data Remote Memory Corruption Vulnerability
11922	Microsoft Windows WINS Name Value Handling Remote Buffer Overflow Vulnerability
11375	Microsoft Windows WMF/EMF Image Format Rendering Remote Buffer Overflow Vulnerability
10120	Microsoft Windows WMF/EMF Image Formats Remote Buffer Overflow Vulnerability
9892	Microsoft Windows XP explorer.exe Remote Denial of Service Vulnerability
5557	Multiple Microsoft Internet Explorer Vulnerabilities
4930	Multiple Microsoft Product Gopher Client Buffer Overflow Vulnerability
9694	Windows NtSystemDebugControl() Kernel API Function Privilege Escalation
13767	GNU SHTool Insecure Temporary File Deletion Vulnerability
2206	PHP .htaccess Attribute Transfer Vulnerability
6557	PHP 4.0.3 IMAP Module Buffer Overflow Vulnerability
16220	PHP 5 User-Supplied Session ID Input Validation Vulnerability
15177	PHP Apache 2 Local Denial of Service Vulnerability
15413	PHP Apache 2 Virtual() Safe_Mode and Open_Basedir Restriction Bypass Vulnerability
7256	PHP array_pad() Integer Overflow Memory Corruption Vulnerability
6875	PHP CGI SAPI Code Execution Vulnerability
15411	PHP cURL and GD Multiple Safe_Mode and Open_Basedir Restriction Bypass Vulnerabilities
11557	PHP cURL Open_Basedir Restriction Bypass Vulnerability
8405	PHP DLOpen Memory Disclosure Vulnerability
7199	PHP emalloc() Unspecified Integer Overflow Memory Corruption Vulnerability

Bugtraq ID	Vulnerability Name
2205	PHP Engine Disable Source Viewing Vulnerability
1786	PHP Error Logging Format String Vulnerability
15250	PHP File Upload GLOBAL Variable Overwrite Vulnerability
5681	PHP Function CRLF Injection Vulnerability
12701	PHP Glob Function Local Information Disclosure Vulnerability
13164	PHP Group Exif Module IFD Nesting Denial Of Service Vulnerability
13163	PHP Group Exif Module IFD Tag Integer Overflow Vulnerability
15358	PHP Group Exif Module Infinite Recursion Denial Of Service Vulnerability
12962	PHP Group PHP Image File Format Remote Denial Of Service Vulnerability
13143	PHP Group PHP Multiple Unspecified Vulnerabilities
12963	PHP Group PHP Remote JPEG File Format Remote Denial Of Service Vulnerability
5669	PHP Header Function Script Injection Vulnerability
5278	PHP HTTP POST Incorrect MIME Header Parsing Vulnerability
4063	PHP Include File Relative Directory Information Disclosure Vulnerability
10427	PHP Input/Ouput Wrapper Remote Include Function Command Execution Weakness
5280	PHP Interpreter Direct Invocation Denial Of Service Vulnerability
11992	PHP JPEG Image Buffer Overflow Vulnerability
5562	PHP Mail Function ASCII Control Character Header Spoofing Vulnerability
15571	PHP MB_Send_Mail TO Argument Header Injection Vulnerability
10725	PHP memory_limit Remote Code Execution Vulnerability
10471	PHP Microsoft Windows Shell Escape Functions Command Execution Vulnerability
4325	PHP Move_Uploaded_File Open_Basedir Circumvention Vulnerability
11964	PHP Multiple Local And Remote Vulnerabilities
11981	PHP Multiple Remote Vulnerabilities

Bugtraq ID	Vulnerability Name
4026	PHP MySQL Safe_Mode Filesystem Circumvention Vulnerability
16145	PHP MySQL_Connect Remote Buffer Overflow Vulnerability
16219	PHP MySQLI Error Logging Remote Format String Vulnerability
17688	PHP MySQLI Error Logging Remote Format String Vulnerability_copy
14957	PHP Open_BaseDir Security Restriction Bypass Vulnerability
7210	PHP openlog() Buffer Overflow Vulnerability
15249	PHP Parse_Str Register_Globals Activation Weakness
11334	PHP PHP_Variables Remote Memory Disclosure Vulnerability
7805	PHP PHPInfo Cross-Site Scripting Vulnerability
15248	PHP PHPInfo Cross-Site Scripting Vulnerability
15248	PHP PHPInfo Cross-Site Scripting Vulnerability
4606	PHP posix_getpwnam / posix_getpwuid safe_mode Circumvention Vulnerability
4183	PHP Post File Upload Buffer Overflow Vulnerabilities
11190	PHP Remote Arbitrary Location File Upload Vulnerability
15119	PHP Safedir Restriction Bypass Vulnerabilities
2954	PHP SafeMode Arbitrary File Execution Vulnerability
14858	PHP Session Handling Local Session Hijacking Vulnerability
12045	PHP Shared Memory Module Offset Memory Corruption Vulnerability
7187	PHP socket_iovec_alloc() Integer Overflow Vulnerability
7197	PHP socket_recv() Signed Integer Memory Corruption Vulnerability
7198	PHP socket_recvfrom() Signed Integer Memory Corruption Vulnerability
7259	PHP STR_Repeat Boundary Condition Error Vulnerability
10724	PHP Strip_Tags() Function Bypass Vulnerability
7761	PHP Transparent Session ID Cross Site Scripting Vulnerability
8201	PHP Undefined Safe_Mode_Include_Dir Safemode Bypass Vulnerability
6488	PHP wordwrap() Heap Corruption Vulnerability
911	PHP3 'safe_mode' Failure Vulnerability

Bugtraq ID	Vulnerability Name
8693	PHP4 Base64_Encode() Integer Overflow Vulnerability
8696	PHP4 Multiple Vulnerabilities
12665	PHP4 Readfile Denial Of Service Vulnerability
3873	PHP4 Session Files Local Information Disclosure Vulnerability
14088	XML-RPC for PHP Remote Code Injection Vulnerability

June 20, 2006 (Security Update 26.05)

This content update for Symantec ESM Network Assessment detects and reports 39 additional vulnerabilities and 160 updated vulnerabilities. The following table includes information about the 39 new vulnerabilities.

Bugtraq ID	Vulnerability Name
4849	Microsoft Active Data Objects Buffer Overflow Vulnerability
5372	Microsoft Data Access Components Buffer Overflow Vulnerability
8455	Microsoft Data Access Components ODBC Buffer Overflow Vulnerability
18303	Microsoft DXImageTransform.Microsoft.Light ActiveX Control Remote Code Execution Vulnerability
1869	"Microsoft Exchange Server Invalid MIME Header charset = """" DoS Vulnerability"
18381	Microsoft Exchange Server Outlook Web Access Script Injection Vulnerability
1476	Microsoft IIS 3.0 .htr Missing Variable Denial of Service Vulnerability
1488	Microsoft IIS 4.0/5.0 Source Fragment Disclosure Vulnerability
3193	Microsoft IIS 5.0 In-Process Table Privelege Elevation Vulnerability
2717	Microsoft IIS FTP Denial of Service Vulnerability
4486	Microsoft IIS HTTP Error Page Cross Site Scripting Vulnerability
4479	Microsoft IIS ISAPI Filter Access Violation Denial of Service Vulnerability
2440	Microsoft IIS Multiple Invalid URL Request DoS Vulnerability

Bugtraq ID	Vulnerability Name
6069	Microsoft IIS Out Of Process Privilege Escalation Vulnerability
3190	Microsoft IIS SSI Buffer Overrun Privelege Elevation Vulnerability
2453	Microsoft IIS WebDAV Denial of Service Vulnerability
17404	Microsoft Internet Explorer Address Bar Spoofing Vulnerability
4411	Microsoft Internet Explorer Cascading Style Sheet File Disclosure Vulnerability
18328	Microsoft Internet Explorer COM Object Instantiation Code Execution Vulnerability Variant
15660	Microsoft Internet Explorer CSS Import Cross-Domain Restriction Bypass Vulnerability
4527	Microsoft Internet Explorer Dialog Same Origin Policy Bypass Vulnerability
18309	Microsoft Internet Explorer HTML Decoding Remote Code Execution Vulnerability
18320	Microsoft Internet Explorer Multipart HTML File Handling Remote Code Execution Vulnerability
18321	Microsoft Internet Explorer Persistent Modal Dialog Window Address Bar Spoofing Vulnerability
3693	Microsoft Internet Explorer Remote File Viewing Vulnerability
17820	Microsoft Internet Explorer Unspecified OBJECT Tag Memory Corruption Variant Vulnerability
654	Microsoft JET/ODBC Patch and RDS Fix Registry Key Vulnerabilities
18359	Microsoft JScript Memory Corruption Vulnerability
9407	Microsoft MDAC Function Broadcast Response Buffer Overrun Vulnerability
18357	Microsoft SMB Driver Local Denial Of Service Vulnerability
18394	Microsoft Windows Malformed ART Image Remote Code Execution Vulnerability
18358	Microsoft Windows Routing and Remote Access RASMAN Registry Remote Code Execution Vulnerability
18325	Microsoft Windows Routing and Remote Access Remote Code Execution Vulnerability

Bugtraq ID	Vulnerability Name
18389	Microsoft Windows RPC Mutual Authentication Service Spoofing Vulnerability
18356	Microsoft Windows SMB Driver Local Privilege Escalation Vulnerability
4205	Microsoft Windows SMTP Service Authorization Bypass Vulnerability
18374	Microsoft Windows TCP/IP Protocol Driver Remote Buffer Overflow Vulnerability
6068	Multiple Microsoft IIS Vulnerabilities
307	NT IIS4 Buffer Overflow Vulnerability

The following table includes information about the 160 updated vulnerabilities.

Bugtraq ID	Vulnerability Name
15067	Microsoft Collaboration Data Objects Remote Buffer Overflow Vulnerability
6214	Microsoft Data Access Components RDS Buffer Overflow Vulnerability
4053	Microsoft Exchange Inappropriate Registry Permissions Vulnerability
924	Microsoft Exchange Server AUTH / XAUTH / AUTHINFO DoS Vulnerabilities
8838	Microsoft Exchange Server Buffer Overflow Vulnerability
17908	Microsoft Exchange Server Calendar Remote Code Execution Vulnerability
13952	Microsoft Exchange Server Outlook Web Access HTML Injection Vulnerability
13118	Microsoft Exchange Server SMTP Extended Verb Buffer Overflow Vulnerability
2463	Microsoft IE Telnet Client File Overwrite Vulnerability
1565	Microsoft IIS 4.0/5.0 File Permission Canonicalization Vulnerability
1191	Microsoft IIS 4.0/5.0 Malformed .htr Request Vulnerability
1193	Microsoft IIS 4.0/5.0 Malformed Filename Request Vulnerability
1578	"Microsoft IIS 5.0 ""Translate: f"" Source Disclosure Vulnerability"
2674	Microsoft IIS 5.0 .printer ISAPI Extension Buffer Overflow Vulnerability

Bugtraq ID	Vulnerability Name
3193	Microsoft IIS 5.0 In-Process Table Privelege Elevation Vulnerability
6072	Microsoft IIS Administrative Pages Cross Site Scripting Vulnerabilities
1806	Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability
4478	Microsoft IIS ASP Server-Side Include Buffer Overflow Vulnerability
4490	Microsoft IIS Chunked Encoding Heap Overflow Variant Vulnerability
4485	Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability
1912	Microsoft IIS Executable File Parsing Vulnerability
4482	Microsoft IIS FTP Connection Status Request Denial of Service Vulnerability
4855	Microsoft IIS HTR Chunked Encoding Transfer Heap Overflow Vulnerability
4474	Microsoft IIS HTR ISAPI Extension Buffer Overflow Vulnerability
4476	Microsoft IIS HTTP Header Field Delimiter Buffer Overflow Vulnerability
4487	Microsoft IIS HTTP Redirect Cross Site Scripting Vulnerability
3195	Microsoft IIS MIME Header Denial of Service Vulnerability
3190	Microsoft IIS SSI Buffer Overrun Privelege Elevation Vulnerability
2719	Microsoft IIS Various Domain User Account Access Vulnerability
3578	Microsoft Internet Explorer Arbitrary File Execution Vulnerability
3867	Microsoft Internet Explorer Arbitrary Program Execution Vulnerability
9109	Microsoft Internet Explorer BackToFramedJPU Cross-Domain Policy Vulnerability
9663	Microsoft Internet Explorer Bitmap Processing Integer Overflow Vulnerability
8454	Microsoft Internet Explorer BR549.DLL ActiveX Control Buffer Overflow Vulnerability
8556	Microsoft Internet Explorer Browser Popup Window Object Type Validation Vulnerability
14511	Microsoft Internet Explorer COM Object Instantiation Buffer Overflow Vulnerability

Bugtraq ID	Vulnerability Name
15827	Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability
15061	Microsoft Internet Explorer COM Object Instantiation Variant Vulnerability
4752	Microsoft Internet Explorer Content-Disposition Handling File Execution Vulnerability
4754	Microsoft Internet Explorer Cookie Content Disclosure Vulnerability
3546	Microsoft Internet Explorer Cookie Disclosure Vulnerability
3513	Microsoft Internet Explorer Cookie Disclosure/Modification Vulnerability
17196	Microsoft Internet Explorer CreateTextRange Remote Code Execution Vulnerability
15823	Microsoft Internet Explorer Dialog Manipulation Vulnerability
17454	Microsoft Internet Explorer Double Byte Character Memory Corruption Vulnerability
11377	Microsoft Internet Explorer Double Byte Character Set Handling Address Bar Spoofing Vulnerability
9629	Microsoft Internet Explorer Double-Null URI Denial Of Service Vulnerability
17455	Microsoft Internet Explorer Erroneous IOleClientSite Data Zone Bypass Vulnerability
9015	Microsoft Internet Explorer ExecCommand Cross-Domain Access Violation Vulnerability
9278	Microsoft Internet Explorer File Download Warning Bypass Vulnerability
9014	Microsoft Internet Explorer Function Pointer Override Cross-Domain Access Violation Vulnerability
11367	Microsoft Internet Explorer Heartbeat ActiveX Control Unspecified Vulnerability
3421	Microsoft Internet Explorer HTTP Request Encoding Vulnerability
15825	Microsoft Internet Explorer HTTPS Proxy Information Disclosure Vulnerability
10973	Microsoft Internet Explorer Implicit Drag and Drop File Installation Vulnerability

Bugtraq ID	Vulnerability Name
11366	Microsoft Internet Explorer Install Engine ActiveX Control Buffer Overflow Vulnerability
9106	Microsoft Internet Explorer Invalid ContentType Cache Directory Location Disclosure Weakness
17450	Microsoft Internet Explorer Invalid HTML Parsing Code Execution Vulnerability
9658	Microsoft Internet Explorer ITS Protocol Zone Bypass Vulnerability
14087	Microsoft Internet Explorer Javaprxy.DLL COM Object Instantiation Heap Overflow Vulnerability
10689	Microsoft Internet Explorer JavaScript Method Assignment Cross-Domain Scripting Vulnerability
13799	Microsoft Internet Explorer JavaScript OnLoad Handler Remote Code Execution Vulnerability
14284	Microsoft Internet Explorer JPEG Image Rendering CMP Fencepost Denial Of Service Vulnerability
14285	Microsoft Internet Explorer JPEG Image Rendering Memory Consumption Denial Of Service Vulnerability
14282	Microsoft Internet Explorer JPEG Image Rendering Unspecified Buffer Overflow Vulnerability
14286	Microsoft Internet Explorer JPEG Image Rendering Unspecified Denial Of Service Vulnerability
4392	Microsoft Internet Explorer Known Local File Script Execution Vulnerability
8530	Microsoft Internet Explorer Malformed GIF Double Free Code Execution Vulnerability
9108	Microsoft Internet Explorer Method Caching Mouse Click Event Hijacking Vulnerability
10473	Microsoft Internet Explorer Modal Dialog Zone Bypass Vulnerability
9009	Microsoft Internet Explorer Mouse Click Event Hijacking Vulnerability
9568	Microsoft Internet Explorer NavigateAndFind() Cross-Zone Policy Vulnerability
7806	Microsoft Internet Explorer OBJECT Tag Buffer Overflow Vulnerability
8456	Microsoft Internet Explorer Object Type Validation Vulnerability

Bugtraq ID	Vulnerability Name
3556	Microsoft Internet Explorer Patch Q312461 Existence Vulnerability
17460	Microsoft Internet Explorer Persistent Window Content Address Bar Spoofing Vulnerability
11381	Microsoft Internet Explorer Plug-in Navigations Handling Address Bar Spoofing Vulnerability
13941	Microsoft Internet Explorer PNG Image Rendering Buffer Overflow Vulnerability
17457	Microsoft Internet Explorer Popup Cross-Domain Information Disclosure Vulnerability
10690	Microsoft Internet Explorer Popup.show Mouse Event Hijacking Vulnerability
17131	Microsoft Internet Explorer Script Action Handler Buffer Overflow Vulnerability
9013	Microsoft Internet Explorer Script URL Cross-Domain Access Violation Vulnerability
11383	Microsoft Internet Explorer Secure Sockets Layer Caching Vulnerability
6961	Microsoft Internet Explorer Self Executing HTML File Vulnerability
9628	Microsoft Internet Explorer Shell: IFrame Cross-Zone Scripting Vulnerability
10816	Microsoft Internet Explorer Style Tag Comment Memory Corruption Vulnerability
13946	Microsoft Internet Explorer Unspecified DigWebX ActiveX Control Vulnerability
13947	Microsoft Internet Explorer Unspecified GIF And BMP Denial Of Service Vulnerability
17181	Microsoft Internet Explorer Unspecified Remote HTA Execution Vulnerability
14515	Microsoft Internet Explorer Unspecified SharePoint Portal Services Log Sink ActiveX Vulnerability
11388	Microsoft Internet Explorer Unspecified showHelp Zone Bypass Vulnerability
11466	Microsoft Internet Explorer Valid File Drag and Drop Embedded Code Vulnerability

Bugtraq ID	Vulnerability Name
14512	Microsoft Internet Explorer Web Folder Behaviors Cross-Domain Scripting Vulnerability
9769	Microsoft Internet Explorer window.open Media Bar Cross-Zone Scripting Vulnerability
9798	Microsoft Internet Explorer window.open Search Pane Cross-Zone Scripting Vulnerability
16516	Microsoft Internet Explorer WMF Image Parsing Memory Corruption Vulnerability
9012	Microsoft Internet Explorer XML Object Zone Restriction Bypass Vulnerability
8565	Microsoft Internet Explorer XML Page Object Type Validation Vulnerability
13943	Microsoft Internet Explorer XML Redirect Information Disclosure Vulnerability
8457	Microsoft Internet Explorer Zone Restriction Bypass Script Execution Vulnerability
3420	Microsoft Internet Explorer Zone Spoofing Vulnerability
4753	Microsoft Internet Explorer Zone Spoofing Vulnerability
17462	Microsoft MDAC RDS.Dataspace ActiveX Control Remote Code Execution Vulnerability
15057	Microsoft MSDTC COM+ Remote Code Execution Vulnerability
15058	Microsoft MSDTC TIP Denial Of Service Vulnerability
15059	Microsoft MSDTC TIP Distributed Denial Of Service Vulnerability
1882	Microsoft Network Monitor Multiple Buffer Overflow Vulnerabilities
10711	Microsoft Outlook Express Malformed Email Header Denial Of Service Vulnerability
9105	Microsoft Outlook Express MHTML Forced File Execution Vulnerability
9107	Microsoft Outlook Express MHTML Redirection Local File Parsing Vulnerability
13951	Microsoft Outlook Express NNTP Response Parsing Buffer Overflow Vulnerability
17459	Microsoft Outlook Express Windows Address Book File Parsing Buffer Overflow Vulnerability

Bugtraq ID	Vulnerability Name
2048	Microsoft PhoneBook Server Buffer Overflow
4387	Microsoft Temporary Internet File Execution Vulnerability
14594	Microsoft Visual Studio .NET msdds.dll Remote Code Execution Vulnerability
11378	Microsoft Window Management API Local Privilege Escalation Vulnerability
2394	Microsoft Windows 2000 Domain Controller DoS Vulnerability
15826	Microsoft Windows Asynchronous Procedure Call Local Privilege Escalation Vulnerability
16194	Microsoft Windows Embedded Web Font Buffer Overflow Vulnerability
15064	Microsoft Windows Explorer Web View Script Injection Vulnerability
16074	Microsoft Windows Graphics Rendering Engine WMF SetAbortProc Code Execution Vulnerability
10119	Microsoft Windows Help And Support Center URI Validation Code Execution Vulnerability
5872	Microsoft Windows Help Facilities Vulnerabilities
5874	Microsoft Windows Help Facility ActiveX Control Buffer Overflow Vulnerability
8016	Microsoft Windows HTML Converter HR Align Buffer Overflow Vulnerability
9624	Microsoft Windows Internet Naming Service Buffer Overflow Vulnerability
13116	Microsoft Windows Internet Protocol Validation Remote Code Execution Vulnerability
14519	Microsoft Windows Kerberos Denial Of Service Vulnerability
14520	Microsoft Windows Kerberos PKINIT Man In The Middle Vulnerability
11369	Microsoft Windows Kernel Virtual DOS Machine Privilege Escalation Vulnerability
12481	Microsoft Windows License Logging Service Buffer Overflow Vulnerability
15070	Microsoft Windows Malicious Shortcut Handling Remote Code Execution Variant Vulnerability

Bugtraq ID	Vulnerability Name
15069	Microsoft Windows Malicious Shortcut Handling Remote Code Execution Vulnerability
7640	Microsoft Windows Media Player Automatic File Download and Execution Vulnerability
8263	Microsoft Windows Media Player IE Zone Access Control Bypass Vulnerability
8035	Microsoft Windows Media Services NSIISlog.DLL Remote Buffer Overflow Vulnerability
17905	Microsoft Windows MSDTC Heap Buffer Overflow Vulnerability
17906	Microsoft Windows MSDTC Invalid Memory Access Denial Of Service Vulnerability
15056	Microsoft Windows MSDTC Memory Corruption Vulnerability
11372	Microsoft Windows NetDDE Remote Buffer Overflow Vulnerability
15065	Microsoft Windows Plug And Play UMPNPMGR.DLL wsprintfW Buffer Overflow Vulnerability
10677	Microsoft Windows Program Group Converter Filename Local Buffer Overrun Vulnerability
7146	Microsoft Windows Script Engine JScript.DLL Heap Overflow Vulnerability
12484	Microsoft Windows Server Message Block Handlers Remote Buffer Overflow Vulnerability
10213	Microsoft Windows Shell Long Share Name Buffer Overrun Vulnerability
14518	Microsoft Windows Telephony Service Buffer Overflow Vulnerability
3997	Microsoft Windows Trusted Domain Privilege Escalation Vulnerability
11375	Microsoft Windows WMF/EMF Image Format Rendering Remote Buffer Overflow Vulnerability
3887	Microsoft Windows XP Pro Upgrade IE Patch Downgrade Vulnerability
2708	MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability
2906	MS Visual Studio RAD Support Buffer Overflow Vulnerability
9182	Multiple Browser URI Display Obfuscation Weakness
8577	Multiple Microsoft Internet Explorer Script Execution Vulnerabilities

Bugtraq ID	Vulnerability Name
9841	Multiple Vendor Internet Browser Cookie Path Argument Restriction Bypass Vulnerability
10183	Multiple Vendor TCP Sequence Number Approximation Vulnerability
13124	Multiple Vendor TCP/IP Implementation ICMP Remote Denial Of Service Vulnerabilities
13940	Multiple Vendor Telnet Client Remote Information Disclosure Vulnerability
567	NT Exchange Server Encapsulated SMTP Address Vulnerability
529	NT IIS MDAC RDS Vulnerability
4410	Windows 2000 DCOM Client Memory Disclosure Vulnerability

May 17, 2006 (Security Update 26.03)

This content update for Symantec ESM Network Assessment detects and reports 34 additional vulnerabilities and 4 updated vulnerabilities. The following table includes information about the 34 new vulnerabilities.

Bugtraq ID	Vulnerability Name
15332	Macromedia Flash Array Index Memory Access Vulnerability
17106	Macromedia Flash Multiple Unspecified Security Vulnerabilities
12427	Microsoft Internet Explorer AddChannel Cross-Zone Scripting Vulnerability
13117	Microsoft Internet Explorer Content Advisor File Handling Buffer Overflow Vulnerability
4085	Microsoft Internet Explorer Content-Type Field Arbitrary File Execution Vulnerability
12475	Microsoft Internet Explorer DHTML Method Buffer Overflow Vulnerability
13120	Microsoft Internet Explorer DHTML Object Race Condition Memory Corruption Vulnerability
5561	Microsoft Internet Explorer Dialog Same Origin Policy Bypass Variant Vulnerability

Bugtraq ID	Vulnerability Name
6306	Microsoft Internet Explorer Dialog Style Same Origin Policy Bypass Vulnerability
5559	Microsoft Internet Explorer Download Dialogue File Source Obfuscation Vulnerability
6749	Microsoft Internet Explorer dragDrop Method Local File Reading Vulnerability
3767	Microsoft Internet Explorer GetObject File Disclosure Vulnerability
4080	Microsoft Internet Explorer HTML Document Directive Buffer Overflow Vulnerability
5610	Microsoft Internet Explorer HTML Same Origin Policy Violation Vulnerability
5672	Microsoft Internet Explorer IFrame/Frame Cross-Site/Zone Script Execution Vulnerability
5558	Microsoft Internet Explorer Legacy Text Formatting ActiveX Component Buffer Overflow Vulnerability
13123	Microsoft Internet Explorer Malformed URI Buffer Overflow Vulnerability
6217	Microsoft Internet Explorer Object Tag Temporary Internet File Folder Vulnerability
6216	Microsoft Internet Explorer PNG Buffer Overflow Vulnerability
6366	Microsoft Internet Explorer PNG Deflate Heap Corruption Vulnerability
6961	Microsoft Internet Explorer Self Executing HTML File Vulnerability
3597	Microsoft Internet Explorer Spoofable File Extensions Vulnerability
12477	Microsoft Internet Explorer Unspecified ActiveX Image Control Vulnerability
12473	Microsoft Internet Explorer URI Decoding Vulnerability
11466	Microsoft Internet Explorer Valid File Drag and Drop Embedded Code Vulnerability
5560	Microsoft Internet Explorer XML Redirect File Disclosure Vulnerability
8016	Microsoft Windows HTML Converter HR Align Buffer Overflow Vulnerability
8035	Microsoft Windows Media Services NSIISlog.DLL Remote Buffer Overflow Vulnerability

Bugtraq ID	Vulnerability Name
17905	Microsoft Windows MSDTC Heap Buffer Overflow Vulnerability
17906	Microsoft Windows MSDTC Invalid Memory Access Denial Of Service Vulnerability
7146	Microsoft Windows Script Engine JScript.DLL Heap Overflow Vulnerability
10517	Multiple Browser URI Obfuscation Weakness
5557	Multiple Microsoft Internet Explorer Vulnerabilities
4930	Multiple Microsoft Product Gopher Client Buffer Overflow Vulnerability

April 18, 2006 (Security Update 26.01)

This content update for Symantec ESM Network Assessment detects and reports 47 additional vulnerabilities. The following table includes information about the 47 new vulnerabilities.

Bugtraq ID	Vulnerability Name
3138	Oracle DBSNMP Oracle Home Environment Variable Buffer Overflow
4034	Oracle 9IAS OracleJSP Information Disclosure Vulnerability
4391	Oracle 9i TNS Denial of Service Vulnerability
4523	Oracle 9i ANSI Outer Join Access Control Bypass Vulnerability
4845	Oracle TNSListener SERVICE_NAME Remote Buffer Overflow Vulnerability
6085	Oracle 9i Database Server iSQL Plus Malformed USERID Buffer Overflow Vulnerability
6414	Oracle Startup Script LD_LIBRARY_PATH Vulnerability
7395	Oracle9iAS Web Cache Administration Interface Plaintext Password Vulnerability
8375	Multiple Oracle XDB FTP / HTTP Services Buffer Overflow Vulnerabilities
8844	Oracle Database Server Oracle Binary Local Buffer Overflow Vulnerability
8845	Oracle Database Server OracleO Binary Local Buffer Overflow Vulnerability

Bugtraq ID	Vulnerability Name
9587	Multiple Oracle Database Parameter/Statement Buffer Overflow Vulnerabilities
9703	Oracle 9i Application/Database Server SOAP XML DTD Denial Of Service Vulnerability
9705	Oracle9i Database Server Unspecified Security Vulnerabilities
10363	Microsoft Windows XP Self-Executing Folder Vulnerability
10656	Oracle Database 10g Installer Insecure Temporary File Creation Vulnerability
11091	Oracle 10g Database DBMS_SCHEDULER Remote Command Execution Vulnerability
11120	Oracle Database 9i SQL Command Buffer Overflow Vulnerability
12296	Oracle Database Multiple Unspecified Vulnerabilities
13145	Oracle Database MDSYS.MD2.SDO_CODE_SIZE Buffer Overflow Vulnerability
13234	Oracle Database Server CREATE_SCN_CHANGE_SET Standard Procedure SQL Injection Vulnerability
13235	Oracle Database Server ALTER_MANUALLOG_CHANGE_SOURCE SQL Injection Vulnerability
13236	Oracle 10g Database SUBSCRIPTION_NAME Remote SQL Injection Vulnerability
13238	Oracle 9i/10g Database OBJECT_TYPE Remote SQL Injection Vulnerability
13239	Oracle Database Server InterMedia Denial of Service Vulnerability
13509	Oracle 10g DBMS_Scheduler Privilege Escalation Vulnerability
13510	Oracle 9i/10g Database Fine Grained Audit Logging Failure Vulnerability
14281	Oracle9i 9.0.1.5 FIPS Single Sign-On Server Unspecified Cross-Site Scripting Vulnerability
15030	Oracle iSQLPlus Cross-Site Scripting Vulnerability
15032	Oracle iSQL*Plus TLS Listener Remote Denial Of Service Vulnerability
15034	Oracle XML DB Cross-Site Scripting Vulnerability
16287	Oracle January Security Update Multiple Vulnerabilities

Bugtraq ID	Vulnerability Name
16294	Oracle Database SYS.KUPV$FT Multiple SQL Injection Vulnerabilities
16516	Microsoft Internet Explorer WMF Image Parsing Memory Corruption Vulnerability
17131	Microsoft Internet Explorer Script Action Handler Buffer Overflow Vulnerability
17181	Microsoft Internet Explorer Unspecified Remote HTA Execution Vulnerability
17196	Microsoft Internet Explorer CreateTextRange Remote Code Execution Vulnerability
17426	Oracle Database Access Restriction Bypass Vulnerability
17450	Microsoft Internet Explorer Invalid HTML Parsing Code Execution Vulnerability
17453	Microsoft Internet Explorer COM Object Instantiation Code Execution Vulnerability
17454	Microsoft Internet Explorer Double Byte Character Memory Corruption Vulnerability
17455	Microsoft Internet Explorer Erroneous IOleClientSite Data Zone Bypass Vulnerability
17457	Microsoft Internet Explorer Popup Cross-Domain Information Disclosure Vulnerability
17459	Microsoft Outlook Express Windows Address Book File Parsing Buffer Overflow Vulnerability
17460	Microsoft Internet Explorer Persistent Window Content Address Bar Spoofing Vulnerability
17462	Microsoft MDAC RDS.Dataspace ActiveX Control Remote Code Execution Vulnerability
17464	Microsoft Windows Shell COM Object Remote Code Execution Vulnerability

March 22, 2006 (Security Update 25.04)

This content update for Symantec ESM Network Assessment detects and reports 57 additional vulnerabilities and 24 updated vulnerabilities. The following table includes information about the 57 new vulnerabilities.

Bugtraq ID	Vulnerability Name
159	Oracle 8 oratclsh Suid Vulnerability
170	Oracle 8 File Access Vulnerabilities
1035	Oracle for Linux Installer Vulnerability
1828	Oracle Internet Directory 2.0.6 oidldap Vulnerability
1968	Oracle cmctl Buffer Overflow Vulnerability
2295	Oracle XSQL Servlet Arbitrary Java Code Vulnerability
2941	Oracle 8i TNS Listener Buffer Overflow Vulnerability
3135	Oracle /tmp Race Condition Vulnerability
3139	Oracle OTRCREP Oracle Home Environment Variable Buffer Overflow Vulnerability
3381	WinMySQLadmin Plain Text Password Storage Vulnerability
3899	Oracle RDBMS Server Default Account Vulnerability
3900	Oracle SQL*Plus Unauthorized Shell Command Execution Vulnerability
3902	Oracle Database Auditing Insecure Default Configuration Vulnerability
3903	Oracle 8i dbsnmp Command Remote Denial of Service Vulnerability
4032	Oracle 9iAS Apache PL/SQL Module Multiple Buffer Overflows Vulnerability
4037	Oracle 9iAS Apache PL/SQL Module Denial of Service Vulnerability
4290	Oracle 9i Default Configuration File Information Disclosure Vulnerability
4292	Oracle 9iAS Apache PL/SQL Module Web Administration Access Vulnerability
4413	Oracle 8i TNS Listener Local Command Parameter Buffer Overflow Vulnerability
5457	Oracle Listener Malformed Debugging Command Denial Of Service Vulnerability

Bugtraq ID	Vulnerability Name
5460	Oracle Net Listener Format String Vulnerability
5678	Oracle TNS Listener Service_CurLoad Remote Denial Of Service Vulnerability
6733	Oracle 8i Listener Remote Redirect Denial of Service Vulnerability
6847	Oracle Database Server TO_TIMESTAMP_TZ Buffer Overflow Vulnerability
6848	Oracle Database Server TZ_OFFSET Buffer Overflow Vulnerability
6850	Oracle Database Server DIRECTORY Buffer Overflow Vulnerability
7453	Oracle Net Services Link Buffer Overflow Vulnerability
8267	Oracle Database Server EXTPROC Buffer Overflow Vulnerability
9976	MySQL Aborted Bug Report Insecure Temporary File Creation Vulnerability
10142	MySQL MYSQLD_Multi Insecure Temporary File Creation Vulnerability
10654	MySQL Authentication Bypass Vulnerability
10655	MySQL Password Length Remote Buffer Overflow Vulnerability
10829	Oracle Database Default Library Directory Privilege Escalation Vulnerability
10871	Oracle Multiple Unspecified Vulnerabilities
10969	MySQL Mysqlhotcopy Script Insecure Temporary File Creation Vulnerability
11099	Oracle Database Server ctxsys.driload Access Validation Vulnerability
11100	Oracle Database Server dbms_system.ksdwrt Remote Buffer Overflow Vulnerability
11261	MySQL Bounded Parameter Statement Execution Remote Buffer Overflow Vulnerability
11291	MySQL Unspecified Insecure Temporary File Creation Vulnerability
11357	MySQL Multiple Local Vulnerabilities
11432	MySQL Remote FULLTEXT Search Denial Of Service Vulnerability
11435	MySQL Database Unauthorized GRANT Privilege Vulnerability
11726	Sun Java Runtime Environment Java Plug-in JavaScript Security Restriction Bypass Vulnerability

Bugtraq ID	Vulnerability Name
12277	MySQL Database MySQLAccess Local Insecure Temporary File Creation Vulnerability
12301	Oracle Database Multiple Vulnerabilities
12749	Oracle Database 8i/9i Multiple Remote Directory Traversal Vulnerabilities
12781	MySQL AB MySQL Multiple Remote Vulnerabilities
13139	Oracle Multiple Vulnerabilities
13144	Oracle Database Multiple SQL Injection Vulnerabilities
13660	MySQL mysql_install_db Insecure Temporary File Creation Vulnerability
14162	Zlib Compression Library Buffer Overflow Vulnerability
14238	Oracle July Security Update Multiple Vulnerabilities
14509	MySQL User-Defined Function Buffer Overflow Vulnerability
15134	Oracle October Security Update Multiple Vulnerabilities
15450	Oracle Database Windows XP Simple File Sharing Authentication Bypass Vulnerability
16484	Microsoft Windows Multiple Local Privilege Escalation Vulnerabilities
16850	MySQL Query Logging Bypass Vulnerability

February 23, 2006 (Security Update 25.03)

This content update for Symantec ESM Network Assessment detects and reports 60 additional vulnerabilities. The following table includes information about the 60 new vulnerabilities.

Bugtraq ID	Vulnerability Name
911	PHP3 'safe_mode' Failure Vulnerability
1161	Cisco Router Online Help Vulnerability
1786	PHP Error Logging Format String Vulnerability
2205	PHP Engine Disable Source Viewing Vulnerability
2206	PHP .htaccess Attribute Transfer Vulnerability

Bugtraq ID	Vulnerability Name
3873	PHP4 Session Files Local Information Disclosure Vulnerability
4063	PHP Include File Relative Directory Information Disclosure Vulnerability
4325	PHP Move_Uploaded_File Open_Basedir Circumvention Vulnerability
4387	Microsoft Temporary Internet File Execution Vulnerability
4606	PHP posix_getpwnam / posix_getpwuid safe_mode Circumvention Vulnerability
5280	PHP Interpreter Direct Invocation Denial Of Service Vulnerability
5669	PHP Header Function Script Injection Vulnerability
5681	PHP Function CRLF Injection Vulnerability
5872	Microsoft Windows Help Facilities Vulnerabilities
8201	PHP Undefined Safe_Mode_Include_Dir Safemode Bypass Vulnerability
8405	PHP DLOpen Memory Disclosure Vulnerability
8693	PHP4 Base64_Encode() Integer Overflow Vulnerability
8696	PHP4 Multiple Vulnerabilities
10427	PHP Input/Output Wrapper Remote Include Function Command Execution Weakness
10471	PHP Microsoft Windows Shell Escape Functions Command Execution Vulnerability
11190	PHP Remote Arbitrary Location File Upload Vulnerability
11334	PHP PHP_Variables Remote Memory Disclosure Vulnerability
11557	PHP cURL Open_Basedir Restriction Bypass Vulnerability
11964	PHP Multiple Local And Remote Vulnerabilities
11981	PHP Multiple Remote Vulnerabilities
11992	PHP JPEG Image Buffer Overflow Vulnerability
12045	PHP Shared Memory Module Offset Memory Corruption Vulnerability
12307	Cisco IOS Skinny Call Control Protocol Handler Remote Denial Of Service Vulnerability
12665	PHP4 Readfile Denial Of Service Vulnerability
12701	PHP Glob Function Local Information Disclosure Vulnerability

Bugtraq ID	Vulnerability Name
12962	PHP Group PHP Image File Format Remote Denial Of Service Vulnerability
12963	PHP Group PHP Remote JPEG File Format Remote Denial Of Service Vulnerability
13143	PHP Group PHP Multiple Unspecified Vulnerabilities
13163	PHP Group Exif Module IFD Tag Integer Overflow Vulnerability
13164	PHP Group Exif Module IFD Nesting Denial Of Service Vulnerability
13767	GNU SHTool Insecure Temporary File Deletion Vulnerability
14088	XML-RPC for PHP Remote Code Injection Vulnerability
14858	PHP Session Handling Local Session Hijacking Vulnerability
14957	PHP Open_BaseDir Security Restriction Bypass Vulnerability
15119	PHP Safedir Restriction Bypass Vulnerabilities
15177	PHP Apache 2 Local Denial of Service Vulnerability
15248	PHP PHPInfo Cross-Site Scripting Vulnerability
15249	PHP Parse_Str Register_Globals Activation Weakness
15250	PHP File Upload GLOBAL Variable Overwrite Vulnerability
15358	PHP Group Exif Module Infinite Recursion Denial Of Service Vulnerability
15411	PHP cURL and GD Multiple Safe_Mode and Open_Basedir Restriction Bypass Vulnerabilities
15413	PHP Apache 2 Virtual() Safe_Mode and Open_Basedir Restriction Bypass Vulnerability
15571	PHP MB_Send_Mail TO Argument Header Injection Vulnerability
15602	Cisco IOS HTTP Service HTML Injection Vulnerability
15762	Apache MPM Worker.C Denial Of Service Vulnerability
15834	Apache Mod_IMAP Referer Cross-Site Scripting Vulnerability
16145	PHP MySQL_Connect Remote Buffer Overflow Vulnerability
16152	Apache Mod_SSL Custom Error Document Remote Denial Of Service Vulnerability
16219	PHP MySQLI Error Logging Remote Format String Vulnerability

Bugtraq ID	Vulnerability Name
16220	PHP 5 User-Supplied Session ID Input Validation Vulnerability
16291	Cisco IOS HTTP Service CDP Status Page HTML Injection Vulnerability
16303	Cisco IOS SGBP Remote Denial of Service Vulnerability
16383	Cisco IOS TCLSH AAA Command Authorization Bypass Vulnerability
16636	Microsoft Windows Web Client Buffer Overflow Vulnerability
16645	Microsoft Windows IGMPv3 Denial of Service Vulnerability

January 18, 2006 (Security Update 25.02)

This content update for Symantec ESM Network Assessment detects and reports 30 additional vulnerabilities. The following table includes information about the 30 new vulnerabilities.

Bugtraq ID	Vulnerability Name
1882	Microsoft Network Monitor Multiple Buffer Overflow Vulnerabilities
2022	Multiple Vendor TCP/IP Resource Exhaustion Vulnerability
2048	Microsoft PhoneBook Server Buffer Overflow
2906	MS Visual Studio RAD Support Buffer Overflow Vulnerability
3513	Microsoft Internet Explorer Cookie Disclosure/Modification Vulnerability
3546	Microsoft Internet Explorer Cookie Disclosure Vulnerability
3556	Microsoft Internet Explorer Patch Q312461 Existence Vulnerability
3723	Microsoft UPnP NOTIFY Buffer Overflow Vulnerability
3724	Microsoft Universal Plug and Play Simple Service Discovery Protocol Denial of Service Vulnerability
3997	Microsoft Windows Trusted Domain Privilege Escalation Vulnerability
4410	Windows 2000 DCOM Client Memory Disclosure Vulnerability
5874	Microsoft Windows Help Facility ActiveX Control Buffer Overflow Vulnerability
10111	Microsoft Windows H.323 Remote Buffer Overflow Vulnerability
10113	Microsoft Negotiate SSP Remote Buffer Overflow Vulnerability

Bugtraq ID	Vulnerability Name
10114	Microsoft Windows 2000 Domain Controller LDAP Denial Of Service Vulnerability
10115	Microsoft Windows SSL Library Denial of Service Vulnerability
10116	Microsoft Windows Private Communications Transport Protocol Buffer Overrun Vulnerability
10117	Microsoft Virtual DOS Machine Local Privilege Escalation Vulnerability
10118	Microsoft ASN.1 Library Double Free Memory Corruption Vulnerability
10120	Microsoft Windows WMF/EMF Image Formats Remote Buffer Overflow Vulnerability
10122	Microsoft Windows Local Descriptor Table Local Privilege Escalation Vulnerability
10124	Microsoft Windows Utility Manager Local Privilege Escalation Vulnerability
11173	Microsoft GDI+ Library JPEG Segment Length Integer Underflow Vulnerability
11379	Microsoft NNTP Component Heap Overflow Vulnerability
11763	Microsoft Windows WINS Association Context Data Remote Memory Corruption Vulnerability
11922	Microsoft Windows WINS Name Value Handling Remote Buffer Overflow Vulnerability
12481	Microsoft Windows License Logging Service Buffer Overflow Vulnerability
12484	Microsoft Windows Server Message Block Handlers Remote Buffer Overflow Vulnerability
16074	Microsoft Windows Graphics Rendering Engine WMF SetAbortProc Code Execution Vulnerability
16194	Microsoft Windows Embedded Web Font Buffer Overflow Vulnerability

December 22, 2005 (Security Update 25.01)

This content update for Symantec ESM Network Assessment detects and reports 54 additional vulnerabilities. The following table includes information about the 54 new vulnerabilities.

Bugtraq ID	Vulnerability Name
1548	Apache Jakarta-Tomcat /admin Context Vulnerability
2518	Apache Tomcat 3.0 Directory Traversal Vulnerability
1531	Apache Tomcat 3.1 Path Revealing Vulnerability
5194	Apache Tomcat DOS Device Name Cross Site Scripting Vulnerability
13756	Apache Tomcat Java Security Manager Bypass Vulnerability
8824	Apache Tomcat Non-HTTP Request Denial Of Service Vulnerability
12795	Apache Tomcat Remote Malformed Request Denial Of Service Vulnerability
15325	Apache Tomcat Simultaneous Directory Listing Denial Of Service Vulnerability
1532	Apache Tomcat Snoop Servlet Information Disclosure Vulnerability
3542	Cisco Access Control List Fragment Keyword Ignored Vulnerability
53	Cisco Access List Vulnerability
8290	Cisco Aironet AP1x00 Malformed HTTP GET Denial Of Service Vulnerability
8292	Cisco Aironet Telnet Service User Account Enumeration Weakness
6059	Cisco AS5350 Universal Gateway Portscan Denial Of Service Vulnerability
10186	Cisco Internet Operating System SNMP Message Processing Denial Of Service Vulnerability
4947	Cisco IOS 12.1 Large TCP Scan Denial of Service Vulnerability
14092	Cisco IOS AAA RADIUS Authentication Bypass Vulnerability
10560	Cisco IOS Border Gateway Protocol Denial Of Service Vulnerability
12370	Cisco IOS Border Gateway Protocol Processing Remote Denial Of Service Vulnerability
11649	Cisco IOS DHCP Input Queue Blocking Denial Of Service Vulnerability
13031	Cisco IOS Easy VPN Server XAUTH Authentication Bypass Vulnerability

Bugtraq ID	Vulnerability Name
14770	Cisco IOS Firewall Authentication Proxy Buffer Overflow Vulnerability
14414	Cisco IOS IPv6 Processing Arbitrary Code Execution Vulnerability
12368	Cisco IOS IPv6 Processing Remote Denial Of Service Vulnerability
12369	Cisco IOS Multi Protocol Label Switching Remote Denial Of Service Vulnerability
10971	Cisco IOS OSPF Remote Denial Of Service Vulnerability
13042	Cisco IOS Secure Shell Server Memory Leak Denial Of Service Vulnerability
13043	Cisco IOS Secure Shell Server V2 Remote Denial Of Service Vulnerability
15275	Cisco IOS System Timers Heap Buffer Overflow Exploitation
13033	Cisco IOS Unauthorized Security Association Establishment Vulnerability
15401	Cisco IPSec Unspecified IKE Traffic Denial Of Service Vulnerabilities
4948	Cisco Malformed HSRP Traffic Denial of Service Vulnerability
4132	Cisco Malformed SNMP Message Denial of Service Vulnerabilities
6358	Cisco OSM Line Cards Denial Of Service Vulnerability
690	Cisco PIX and CBAC Fragmentation Attack
4949	Cisco Spoofed HSRP Loopback Denial Of Service Vulnerability
5041	Cisco uBR7200 / uBR7100 Universal Broadband Routers DOCSIS MIC Bypass Vulnerability
5030	Cisco View-based Access Control MIB SNMP Walk Read-Write Password Revealing Vulnerability
3199	Jakarta Tomcat Error Message Information Disclosure Vulnerability
15827	Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability
15823	Microsoft Internet Explorer Dialog Manipulation Vulnerability
15825	Microsoft Internet Explorer HTTPS Proxy Information Disclosure Vulnerability
13799	Microsoft Internet Explorer JavaScript OnLoad Handler Remote Code Execution Vulnerability
15826	Microsoft Windows Asynchronous Procedure Call Local Privilege Escalation Vulnerability

Bugtraq ID	Vulnerability Name
9406	Multiple Vendor H.323 Protocol Implementation Vulnerabilities
986	Multiple Vendor SNMP World Writeable Community Vulnerability
6408	Multiple Vendor SSH2 Implementation Empty Elements / Multiple Separator Vulnerabilities
6405	Multiple Vendor SSH2 Implementation Incorrect Field Length Vulnerabilities
6410	Multiple Vendor SSH2 Implementation Null Character Handling Vulnerabilities
2682	Multiple Vendor TCP Initial Sequence Number Statistical Vulnerability
2527	Multiple Vendor URL JSP Request Source Code Disclosure Vulnerability
8970	OpenSSL ASN.1 Large Recursion Remote Denial Of Service Vulnerability
2344	PKCS #1 Version 1.5 Session Key Retrieval Vulnerability
1294	TACACS+ Protocol Flaws Vulnerabilities

November 11, 2005 (Security Update 24.02)

This content update for Symantec ESM Network Assessment detects and reports 45 additional vulnerabilities. The following table includes information about the 45 new vulnerabilities.

Bugtraq ID	Vulnerability Name
2216	Apache Web Server DoS Vulnerability
2300	NCSA/Apache httpd ScriptAlias Source Retrieval Vulnerability
3009	Apache Possible Directory Index Disclosure Vulnerability
3169	Apache Server Address Disclosure Vulnerability
3176	Apache Mod ReWrite Rules Bypassing Image Linking Vulnerability
3521	Apache mod_usertrack Predictable ID Generation Vulnerability
3790	Apache Non-Existent Log Directory Denial Of Service Vulnerability
3796	Apache HTTP Request Unexpected Behavior Vulnerability
4056	Apache 2 for Windows php.exe Path Disclosure Vulnerability
4057	Apache 2 for Windows OPTIONS request Path Disclosure Vulnerability

Bugtraq ID	Vulnerability Name
4358	Apache Double-Reverse Lookup Log Entry Spoofing Vulnerability
4431	Apache PrintEnv/Test_CGI Script Injection Vulnerability
4437	Apache Error Message Cross-Site Scripting Vulnerability
5992	Apache HTDigest Insecure Temporary File Vulnerability
6117	Apache mod_php File Descriptor Leakage Vulnerability
6320	Apache/Tomcat Mod_JK Chunked Encoding Denial Of Service Vulnerability
8707	Apache htpasswd Password Entropy Weakness
8725	Apache2 MOD_CGI STDERR Denial Of Service Vulnerability
9302	Apache mod_php Module File Descriptor Leakage Vulnerability
9471	Apache mod_perl Module File Descriptor Leakage Vulnerability
9571	Apache mod_digest Client-Supplied Nonce Verification Vulnerability
9599	Apache mod_php Global Variables Information Disclosure Weakness
9804	Multiple Vendor HTTP Response Splitting Vulnerability
9874	Apache HTAccess LIMIT Directive Bypass Configuration Error Weakness
9921	Apache Connection Blocking Denial Of Service Vulnerability
10212	Apache mod_auth Malformed Password Potential Memory Corruption Vulnerability
10355	Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability
10789	Apache mod_userdir Module Information Disclosure Vulnerability
11154	Apache mod_ssl Remote Denial of Service Vulnerability
11185	Apache Mod_DAV LOCK Denial Of Service Vulnerability
11239	Apache Satisfy Directive Access Control Bypass Vulnerability
11360	Apache mod_ssl SSLCipherSuite Restriction Bypass Vulnerability
11471	Apache mod_include Local Buffer Overflow Vulnerability
12308	Apache Utilities Insecure Temporary File Creation Vulnerability
12834	Microsoft Windows Graphical Device Interface Library Denial Of Service Vulnerability

Bugtraq ID	Vulnerability Name
12877	Apache mod_ssl ssl_io_filter_cleanup Remote Denial Of Service Vulnerability
13537	Apache HTDigest Realm Command Line Argument Buffer Overflow Vulnerability
13777	Apache HTPasswd User Command Line Argument Buffer Overflow Vulnerability
13778	Apache HTPasswd Password Command Line Argument Buffer Overflow Vulnerability
13873	Multiple Vendor Multiple HTTP Request Smuggling Vulnerabilities
14366	Apache mod_ssl CRL Handling Off-By-One Buffer Overflow Vulnerability
14620	PCRE Regular Expression Heap Overflow Vulnerability
14660	Apache CGI Byterange Request Denial of Service Vulnerability
15352	Microsoft Windows Graphics Rendering Engine WMF/EMF Format Code Execution Vulnerability
15356	Microsoft Windows Graphics Rendering Engine WMF Format Code Execution Vulnerability

October 19, 2005 (Security Update 24.01)

This content update for Symantec ESM Network Assessment detects and reports 15 additional vulnerabilities and 357 additional security exposures. The following table includes information about the 15 new vulnerabilities.

Bugtraq ID	Vulnerability Name
12160	Microsoft Windows FTP Client Directory Traversal Vulnerability
14260	Microsoft Windows Network Connections Manager Library Local Denial of Service Vulnerability
14594	Microsoft Visual Studio .NET msdds.dll Remote Code Execution Vulnerability
15056	Microsoft Windows MSDTC Memory Corruption Vulnerability
15057	Microsoft MSDTC COM+ Remote Code Execution Vulnerability
15058	Microsoft MSDTC TIP Denial Of Service Vulnerability
15059	Microsoft MSDTC TIP Distributed Denial Of Service Vulnerability

Bugtraq ID	Vulnerability Name
15061	Microsoft Internet Explorer COM Object Instantiation Variant Vulnerability
15063	Microsoft DirectX DirectShow AVI Processing Buffer Overflow Vulnerability
15064	Microsoft Windows Explorer Web View Script Injection Vulnerability
15065	Microsoft Windows Plug And Play UMPNPMGR.DLL wsprintfW Buffer Overflow Vulnerability
15066	Microsoft Windows Client Service For Netware Buffer Overflow Vulnerability
15067	Microsoft Collaboration Data Objects Remote Buffer Overflow Vulnerability
15069	Microsoft Windows Malicious Shortcut Handling Remote Code Execution Vulnerability
15070	Microsoft Windows Malicious Shortcut Handling Remote Code Execution Variant Vulnerability

The following table includes information about the 357 security exposures.

Bugtraq ID	Exposure Title
exp.4	Server can be compromised with physical access
exp.5	Access to a UNIX password file allows user profiling and possible password cracking
exp.6	MCI registry key does not conform to Microsoft-recommended security settings
exp.7	Windows NT password filter is not enabled
exp.8	Password is easy to guess
exp.9	Windows 95 .pwl file uses weak encryption
exp.10	CurrentVersion key has vulnerable default permissions
exp.11	Performance Monitor's Perflib registry key has inappropriate access controls
exp.12	Daytime service lets attackers probe system
exp.13	Poker service lets attackers profile a computer
exp.14	DCOM lets attackers run arbitrary programs remotely

Bugtraq ID	Exposure Title
exp.15	POP services let attackers profile a computer
exp.16	Portmap services let attackers profile a computer
exp.17	Admin user name and password are stored as plain text in registry
exp.18	WinGate allows attack by proxy with default configuration
exp.19	Dictionary service lets attackers profile computers
exp.20	A registry key that lists communication ports has inappropriate access controls
exp.21	Discard service lets attackers profile a computer
exp.22	POSIX subsystem subjects a host computer to Trojan horse attacks
exp.23	DNS denial of service attack is possible
exp.24	Domain Name Service lets attackers profile a network
exp.25	Echo service lets attackers probe a computer
exp.26	EFS service lets attackers profile a computer
exp.27	Password is insecure
exp.28	erlogin service lets attackers profile a computer
exp.29	Print-srv service lets attackers profile a computer
exp.30	Symantec Enterprise Security Manager is not installed
exp.31	No action can be taken when auditing is unavailable
exp.32	Printer service may profile a system for attack
exp.33	exec service allows remote command execution
exp.35	Finger service can be used in denial of service attack
exp.36	Qmaster service may help profile a system for attack
exp.37	Qotd service lets attackers profile a computer
exp.38	Finger service lets attackers execute arbitrary commands as root
exp.39	Finger service lets attackers profile a computer
exp.40	Finger service reveals information about user accounts
exp.41	Queue service may help profile a system for attack

Bugtraq ID	Exposure Title
exp.42	A registry key that configures applications to edit the registry has inappropriate access controls
exp.43	Finger service lists all active users accounts
exp.44	Finger service listing all users currently logged in
exp.45	Registry can be accessed remotely
exp.46	Finger service lists all inactive user accounts
exp.47	Registry files associated with the registry editor allows access to the registry.
exp.48	Remotefs service may help profile a system for attack
exp.49	Remp service may help profile a system for attack
exp.50	Network resource discovery helps identify systems for attack
exp.51	FTP service allows access
exp.52	ICMP replies help profile a system for attack.
exp.53	FTP service allows anonymous users to write to root directory
exp.54	Rje service may help profile a system for attack
exp.55	Rmt service may help profile a system for attack
exp.56	FTP service may create opportunity for attack
exp.57	FTP backdoor in wu-ftpd may allow anonymous root access
exp.58	Windows NT SP1 and SP2 are vulnerable to RPC denial of service attacks
exp.59	RPC registry settings have inappropriate access controls.
exp.60	Run key has inappropriate access controls
exp.61	RunOnce registry key has inappropriate access controls
exp.62	FTP service allows unauthorized file access
exp.63	SAP information may help profile a system for attack
exp.64	Apache version 1.2.4 and earlier are vulnerable to multiple buffer overflow attacks
exp.65	Pandora spoofing attack possible
exp.66	Sendmail 8.8.0-8.8.1 MIEM overflow allows remote root access
exp.67	Sendmail allows information obscuring via long HELO/EHLO

Bugtraq ID	Exposure Title
exp.68	Windows NT application event log can be accessed by the guest account
exp.69	Sendmail versions up to 8.8.0 allows e-mail re-directs
exp.70	Services identifiable by product or version allow them to be profiled for future attacks
exp.71	Sftp service may help profile a system for attack
exp.72	Windows NT security event log can be accessed by the guest account
exp.73	Windows NT guest account can access the system event log
exp.74	A registry key that configures shares has inappropriate access controls
exp.76	SL Mail service is vulnerable to a buffer overflow attack
exp.77	Registry keys under HKEY_LOCAL_MACHINE are vulnerable to attack
exp.78	SL Mail is vulnerable to a denial of service attack
exp.79	SMB can force the use of clear text passwords
exp.80	HP laserjet IP address can be changed without password
exp.82	SMB client message signing disabled
exp.83	SMB server has message signing disabled
exp.84	Finger client script in CGI directory of web server
exp.85	Perl interpreter accessible from web server
exp.87	Web server running
exp.88	SMTP allows user verification with rcpt field
exp.89	SMTP servers that allow mail relaying can be used to produce spam
exp.90	Firewall type identified
exp.91	SMTP servers that connect to clients quickly may facilitate vulnerability probing
exp.92	Service listening on non-standard port
exp.93	Sendmail allows file manipulation through e-mail sent to a decode alias
exp.94	Unexpected service behavior
exp.95	Network printer may be a target for attack
exp.96	Router or switch may be target for attack

Bugtraq ID	Exposure Title
exp.97	Intruder alert not installed
exp.98	Internal DNS information available to public network
exp.99	SMTP EXPN feature allows for username discovery
exp.100	Valid e-mail account obtainable
exp.101	Smtp service lets attackers profile a computer
exp.105	SSH service may help profile a system for attack
exp.106	Sunrpc service may help profile a system for attack
exp.107	Supdup service may help profile a system for attack
exp.108	Internet Explorer 3.0 and 3.01 are vulnerable to attack
exp.109	Internet explorer without year 2000 patch
exp.110	Systat service allows remote system monitoring
exp.111	Internet explorer 4.01 vulnerable to untrusted scripted paste
exp.112	Tcprepo service may help profile a system for attack
exp.113	Internet explorer 4.x security zones not preserved
exp.114	Telnet service communicates in clear text
exp.115	Tempo service may help profile a system for attack
exp.116	Tetrinet service may help profile a system for attack
exp.117	Time service may help profile a system for attack
exp.118	A registry key that configures PostScript fonts has inappropriate access controls
exp.119	A registry key that configures uninstall applications has inappropriate access controls
exp.120	NULL session connections allow user and domain server enumeration
exp.121	A registry key that configures UPS devices has inappropriate access controls
exp.122	Internet explorer 4.x without service pack 1 is vulnerable to attack
exp.123	Internet Relay Chat server lets attackers probe a computer
exp.124	Login dialogs that display the last user to log in facilitate user account attacks

Bugtraq ID	Exposure Title
exp.125	SMB lets anonymous connections read and write to shares
exp.127	Uucp service may help profile a system for attack
exp.128	Uucp-path service may help profile a system for attack.
exp.129	Netware 4.x vulnerable to denial of service attack
exp.130	LanManager passwords use weak encryption
exp.131	Legal notice banner at login makes prosecuting attackers easier
exp.132	Getadmin attack allows users to be added the administrators group
exp.133	Inappropriate registry access controls allow the SNMP community name to be read.
exp.134	Vmnet0 service may help profile a system for attack
exp.135	VNC service could be monitored to profile a computer
exp.136	Volrmmount utility allows shell users to gain root privileges
exp.137	The w service may help profile a system for attack.
exp.138	Whois service may help profile a system for attack
exp.139	Drivers registry key does not conform to Microsoft recommended security settings
exp.140	Apache win32 allows retrieval of files outside of document trees
exp.141	Embedding registry key does not conform to Microsoft recommended security settings
exp.142	Font Drivers registry key does not conform to Microsoft recommended security settings
exp.143	FontCache registry key does not conform to Microsoft recommended security settings
exp.144	Not clearing the Windows page file may provide attackers with sensitive system information.
exp.145	FontMapper registry key does not conform to Microsoft recommended security settings
exp.146	Fonts registry key does not conform to Microsoft recommended security settings
exp.147	FontSubstitutes registry key does not conform to Microsoft recommended security settings

Bugtraq ID	Exposure Title
exp.148	GRE_Initialize registry key does not conform to Microsoft recommended security settings
exp.149	MCI Extensions registry key does not conform to Microsoft recommended security settings
exp.150	Windows NT system caches logon credentials
exp.151	garcon service may allow attackers to profile for future attacks
exp.152	Windows PWL file uses weak encryption
exp.153	Gateway service may allow attackers to profile for future attacks
exp.154	WinGate pop3 proxy server is vulnerable to a buffer overflow
exp.155	Wingate telnet proxy service is vulnerable to a buffer overflow attack
exp.156	hostnames service may allow attackers to profile for future attacks
exp.157	Inappropriate WinLogin registry key access controls may allow trojan applications to be executed.
exp.158	ingreslock service may allow attackers to profile for future attacks
exp.159	iso-tsap service may allow attackers to profile for future attacks
exp.160	kerberos service may allow attackers to profile for future attacks
exp.161	A registry key that configures how 16 bit processes are executed has inappropriate access controls.
exp.162	X400 service may help profile a system for attack
exp.163	X400-snd service may help profile a system for attack.
exp.164	Malformed broadcast packets can cause a denial of service in older NetWare client software
exp.165	Kerberos master service may allow attackers to profile for future attacks
exp.166	NFS allows device creation
exp.167	NFS is vulnerable to directory traversals that grant access to files that are not exported
exp.168	klogin service may allow attackers to profile for future attacks
exp.169	knetd service may allow attackers to profile for future attacks
exp.170	krb_prop service may allow attackers to profile for future attacks
exp.171	kshell service may allow attackers to profile for future attacks

Bugtraq ID	Exposure Title
exp.172	link service may allow attackers to profile for future attacks
exp.173	rlogin service uses plain text passwords
exp.174	NFS allows root access by failing to properly validate UIDs.
exp.175	NFS services that export writable directories are vulnerable to attack.
exp.176	Exporting hosts.equiv and .rhosts files through NFS as writable makes a system vulnerable to attack
exp.177	Exporting hosts.cshrc and .login files through NFS as writable makes a system vulnerable to attack.
exp.178	Exporting .netrc through NFS as writable makes a system vulnerable to attack.
exp.179	Portmap can be used to create NFS mounts.
exp.180	Access to mountd allows access to local and remote file systems.
exp.181	Mountd service allows discovery of network resources.
exp.182	Mountd service may allow NFS client enumeration
exp.183	Mountd service allows directory to be mounted by anyone.
exp.184	NFS mounts that grant access to .netrc files may compromise user passwords.
exp.185	NFS may publish host names when exporting .netrc files.
exp.186	Passwd files that are exported by NFS compromise user account information.
exp.187	Passwd files that are exported by NFS with encrypted passwords compromise user account information.
exp.188	Sendmail is vulnerable to a denial of service attack through a malformed message header.
exp.190	Append actions can overwrite a file in older Linux kernels with securelevel protection enabled.
exp.191	SLmailNT 3.1-3.2 allows file restrictions to be bypassed by users.
exp.192	SLmailNT 3.1 and prior can be terminated by remote users.
exp.193	NIS client can be identified via passwd file.
exp.194	Maitrd service may help profile a system for attack
exp.195	Man service may help profile a system for attack

Bugtraq ID	Exposure Title
exp.196	Mantst service may help profile a system for attack
exp.199	Mtb service may help profile a system for attack
exp.200	Mtp service may help profile a system for attack
exp.201	Name service may help profile a system for attack.
exp.202	Windows NT 4 is vulnerable to a denial of service attack through named pipes.
exp.203	Nameserver service may help profile a system for attack
exp.204	Nbname service may help profile a system for attack.
exp.205	Nbsession service may help profile a system for attack.
exp.206	NetBus backdoor service allows remote attackers system level access.
exp.207	Netnews service may help profile a system for attack.
exp.208	NetWare console grants system level access without authentication.
exp.209	NetWare password intercept possible via trojan horse
exp.210	Netstat service my help profile a system for attack.
exp.211	Rconsole passwords stored in clear text.
exp.212	NetWare serves with DOS loaded allow access to DOS partitions.
exp.213	NetWare telnet server allows insecure remote console access
exp.215	Windows could allow network access to the floppy drive.
exp.216	Networks can be identified through NIS.
exp.217	Network Peripherals switching hub is vulnerable to a denial of service attack.
exp.218	Network Peripherals switching hub's IP address can be changed without a password.
exp.219	NeWS service may help profile a system for attack
exp.220	Windows NT 4.0 is vulnerable to newtear
exp.221	NFS may help profile a system for attack
exp.222	Windows NT 4.0 allows network access to the CD-ROM
exp.223	NIS may help profile a system for attack
exp.224	NIS map ethers.byname may help profile a system for attack

Bugtraq ID	Exposure Title
exp.225	NIS map ethers.byaddr may help profile a system for attack
exp.226	NIS map bootparams may help profile a system for attack.
exp.227	NIS map auto.master may help profile a system for attack
exp.228	NIS map auto.home may help profile a system for attack
exp.229	NIS map auto.direct may help profile a system for attack.
exp.230	NIS map auto.src may help profile a system for attack
exp.231	RPC services let attackers profile a computer
exp.232	Portmap service identifies running RPC services
exp.233	Trinoo agent daemons allow denial of service attacks by proxy.
exp.234	Trinoo master daemons allow denial of service attacks by proxy.
exp.235	Tfn trojan horse daemon allows attack-by-proxy
exp.236	Stacheldraht trojan horse agent allows attack-by-proxy.
exp.237	Stacheldraht trojan horse handler allows attack-by-proxy.
exp.238	Stacheldraht trojan horse component allows attack-by-proxy.
exp.239	Mstream trojan horse master allows attack-by-proxy
exp.240	Mstream server allows attack by proxy.
exp.241	Cold Fusion sourcewindow.cfm allows remote file access
exp.242	Cold Fusion evaluate.cfm may allow unauthorized access
exp.243	Cold Fusion fileexists.cfm allows remote file detection access
exp.244	Cold Fusion sample file cfmlsyntaxcheck.cfm is vulnerable to a denial of service attack.
exp.245	Cold Fusion mainframeset.cfm allows local http access by proxy.
exp.246	Linux kernel capability bug allows shell users to gain root access.
exp.247	Personal Mail Server is vulnerable to a buffer overflow attack
exp.248	University of Washington POP/IMAP server are vulnerable to buffer overflow attacks.
exp.249	Unsigned ActiveX controls marked safe for scripting in Restricted Sites zone
exp.250	Active scripting enabled in Restricted Sites zone

Bugtraq ID	Exposure Title
exp.251	Microsoft Outlook is not in the Restricted Sites zone.
exp.252	Microsoft Outlook Express is not in the Restricted Sites zone.
exp.253	SNMP community names provide write access to MIB entries
exp.254	BIND is vulnerable to a fdmax denial of service attack
exp.255	BIND is vulnerable to a maxdname buffer overflow attack.
exp.257	BIND is vulnerable to a sig denial of service attack.
exp.258	BIND is vulnerable to a solinger denial of service attack.
exp.259	BIND is vulnerable to a sigdiv0 denial of service attack.
exp.260	BIND is vulnerable to a srv denial of service attack.
exp.261	BIND discloses system information.
exp.262	Girlfriend backdoor program listens on port 21554.
exp.263	Deep Throat client grants remote attackers administrative system access.
exp.264	Subseven back door gives administrative control to remote attackers
exp.265	A Jana HTTP server CGI allows directory traversals to reference files outside of the document root.
exp.266	HTTP allows CGI access to config.sys
exp.267	ICQ-WebServer allows access to files outside of the document root.
exp.268	_AuthChangeUrl.cgi allows password attacks by proxy.
exp.269	HTTP allows CGI access to _vti_inf.html
exp.270	HTTP allows CGI access to _vti_pvt/service.grp
exp.271	HTTP allows execution of catalog_type.asp CGI
exp.272	HTTP server allows execution of sendmail.cfm CGI
exp.274	HTTP service allows execution of AnyBoard.cgi CGI
exp.275	HTTP service allows execution of AT-admin.cgi CGI
exp.276	HTTP service allows execution of ax-admin.cgi CGI
exp.277	HTTP service allows execution of ax.cgi CGI
exp.278	HTTP service allows execution of bb-hist.sh CGI
exp.280	HTTP service allows execution of day5datacopier.cgi CGI

Bugtraq ID	Exposure Title
exp.281	HTTP service allows execution of day5datanotifier.cgi CGI
exp.283	HTTP service allows execution of dumpenv.pl CGI
exp.284	HTTP service allows execution of environ.cgi CGI
exp.285	HTTP service allows execution of filemail.pl CGI
exp.288	HTTP service allows execution of fpexplore.exe CGI
exp.289	HTTP service allows execution of gH.cgi CGI
exp.293	HTTP service allows execution of maillist.pl CGI
exp.294	HTTP service allows execution of nph-publish CGI
exp.295	HTTP service allows CGI access to passwd.
exp.296	HTTP service allows CGI access to passwd.pwd
exp.297	HTTP service allows CGI access to passwd.txt.
exp.298	HTTP service allows CGI access to password
exp.299	HTTP service allows CGI access to password.pwd
exp.300	HTTP service allows CGI access to password.pwl
exp.301	HTTP service allows execution of perlshop.cgi CGI
exp.303	HTTP service allows execution of ppdscgi.exe CGI
exp.304	HTTP service allows execution of rwwwshell.pl CGI
exp.305	HTTP service allows execution of sendform.cgi CGI
exp.310	HTTP service allows execution of tst.bat CGI
exp.311	HTTP service allows execution of unlg1.1 CGI
exp.312	HTTP service allows execution of unlg1.2 CGI
exp.313	HTTP service allows execution of upload.pl CGI
exp.318	HTTP service allows execution of wwwadmin.pl CGI
exp.319	HTTP service allows execution of args.bat CGI
exp.320	HTTP service allows execution of args.cmd CGI
exp.321	HTTP service allows execution of default.asp CGI
exp.322	HTTP service allows view of the doc directory.

Bugtraq ID	Exposure Title
exp.323	HTTP service allows execution of domcfg.nsf CGI
exp.324	HTTP service allows access to etc/group
exp.325	HTTP service allows access to etc/passwd
exp.337	HTTP service allows execution of fpcount.exe CGI that is vulnerable to a buffer overflow attack
exp.338	HTTP service allows execution of pfieffer.bat CGI that may help profile the system for attack.
exp.339	HTTP service allows execution of pfieffer.cmd CGI
exp.342	HTTP service allows execution of queryhit.htm CGI
exp.343	HTTP service allows execution of adminlogin CGI
exp.344	HTTP service allows execution of tools/getdrvs.exe CGI
exp.346	NAVCE service not detected
exp.347	NAVCE service Identified
exp.348	Shaft distributed denial of service daemon allows attack by proxy
exp.349	Packaging Anomaly Could Cause Hotfixes to be removed
exp.350	Carbon Copy can provide remote access to a computer
exp.351	CaptureScreen can provide remote access to a computer
exp.352	Desktop Delivery can provide remote access to a computer
exp.353	IKS (Invisible Keylogger Stealth) will keep a log of all keystrokes typed
exp.354	NetBus backdoor program allows remote administrative access.
exp.355	Netlook allows a remote capture of screenshots
exp.356	PC Protect Stealth logs stored locally
exp.357	Serv-U FTP-Server v2.5e is vulnerable to a denial of service attack
exp.358	Serv-U FTP-Server version 2.3x is vulnerable to a buffer overflow attack
exp.360	Microsoft IIS Malformed HTR Request vulnerable to buffer overflow attack
exp.361	Microsoft SQL Server 2000 stored procedure is vulnerable to an input validation attack
exp.362	Microsoft MSSQL server may help profile a system for attack.

Bugtraq ID	Exposure Title
exp.363	Microsoft SQL Server 2000 is vulnerable to a OpenDataSource buffer overflow attack
exp.364	VPN service enabled
exp.365	Embedded web servers may help profile a host for attack
exp.366	Wireless access point may allow unauthorized network access
exp.367	D-Link wireless access point can reveal version information
exp.368	Netgear wireless access point may real version information.
exp.369	SMC wireless access point may reveal version information.
exp.370	Cisco-Aironet Wireless Access Point Identified
exp.371	Corega wireless access point may reveal version information.
exp.372	IOData wireless access point may reveal version information.
exp.373	Melco wireless access point may reveal version information.
exp.374	Melco wireless access point can be identified through SNMP.
exp.375	SESA agent not installed.
exp.376	SESA agent identified.
exp.377	SESA Manager detected.
exp.382	BackOrifice allows remote system access with administrator privileges
exp.391	Unauthorized users can add printer drivers
exp.401	Unauthorized users can shut down system
exp.407	Weak passwords allow compromise
exp.408	Rlogin allows remote root access
exp.409	User rights not being audited
exp.410	Open TCP and UDP port allows system profiling
exp.411	Auth service running
exp.413	Base system objects are not protected from modification
exp.414	Chargen service found to be running
exp.450	System may be susceptible to burn attack
exp.452	Busboy service found to be running

Bugtraq ID	Exposure Title
exp.470	Registry key \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Compatibility
exp.501	Microsoft Windows NULL session logon can enumerate users
exp.503	Registry key \HKEY_USERS\.Default has inappropriate security settings
exp.504	Parent of shared directory can be accessed by remote attacker
exp.505	anonymous FTP access is enabled
exp.506	Windows shares can be enumerated remotely
exp.507	Registry key \HKEY_LOCAL_MACHINE\Software\Classes\AppId has vulnerable default permissions
exp.508	NIS allows user account and system information to be obtained
exp.509	Bnews service found to be running
exp.511	Unnecessary services on a host may present opportunities for attack
exp.512	nntp service may profile a host for attack
exp.514	Registry key for Ole has inappropriate access settings
exp.515	OS/2 subsystem enabled on windows
exp.516	Default user automatically logged in through autologin feature
exp.545	SNMP community name is guessable
exp.547	Remote access to shell interpreters in cgi-bin directory

September 20, 2005 (Security Update 23.04)

This content update for Symantec ESM Network Assessment detects and reports 11 additional vulnerabilities. The following table includes information about the 11 new vulnerabilities.

Bugtraq ID	Vulnerability Name
10183	Multiple Vendor TCP Sequence Number Approximation Vulnerability
13109	Windows Kernel Font Buffer Overflow Vulnerability
13110	Microsoft Windows Kernel Object Management Denial Of Service Vulnerability

Bugtraq ID	Vulnerability Name
13112	Microsoft Windows Message Queuing Remote Buffer Overflow Vulnerability
13115	Microsoft Windows Kernel CSRSS Local Privilege Escalation Vulnerability
13116	Microsoft Windows Internet Protocol Validation Remote Code Execution Vulnerability
13118	Microsoft Exchange Server SMTP Extended Verb Buffer Overflow Vulnerability
13121	Microsoft Windows Kernel Access Validation Request Buffer Overflow Vulnerability
13124	Multiple Vendor TCP/IP Implementation ICMP Remote Denial Of Service Vulnerabilities
13132	Microsoft Windows Shell Remote Code Execution Vulnerability
13248	Microsoft Windows Explorer Preview Pane Script Injection Vulnerability

August 25, 2005 (Security Update 23.03)

This content update for Symantec ESM Network Assessment detects and reports 28 additional vulnerabilities. The following table includes information about the 28 new vulnerabilities.

Bugtraq ID	Vulnerability Name
2323	Microsoft Hotfix Conflict Vulnerability
2463	Microsoft IE Telnet Client File Overwrite Vulnerability
2719	Microsoft IIS Various Domain User Account Access Vulnerability
3195	Microsoft IIS MIME Header Denial of Service Vulnerability
3887	Microsoft Windows XP Pro Upgrade IE Patch Downgrade Vulnerability
4087	Microsoft Internet Explorer MIME Type File Extension Spoofing Vulnerability
4392	Microsoft Internet Explorer Known Local File Script Execution Vulnerability
4487	Microsoft IIS HTTP Redirect Cross Site Scripting Vulnerability
4754	Microsoft Internet Explorer Cookie Content Disclosure Vulnerability

Bugtraq ID	Vulnerability Name
6072	Microsoft IIS Administrative Pages Cross Site Scripting Vulnerabilities
9011	Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability
10112	Microsoft Jet Database Engine Remote Code Execution Vulnerability
10126	Microsoft Windows Logon Process Remote Buffer Overflow Vulnerability
10321	Microsoft Windows HSC DVD Driver Upgrade Code Execution Vulnerability
13300	Microsoft Windows ASN.1 Library Bit String Processing Variant Heap Corruption Vulnerability
14259	Microsoft Windows Kernel Unspecified Remote Desktop Protocol Denial Of Service Vulnerability
14282	Microsoft Internet Explorer JPEG Image Rendering Unspecified Buffer Overflow Vulnerability
14284	Microsoft Internet Explorer JPEG Image Rendering CMP Fencepost Denial Of Service Vulnerability
14285	Microsoft Internet Explorer JPEG Image Rendering Memory Consumption Denial Of Service Vulnerability
14286	Microsoft Internet Explorer JPEG Image Rendering Unspecified Denial Of Service Vulnerability
14511	Microsoft Internet Explorer COM Object Instantiation Buffer Overflow Vulnerability
14512	Microsoft Internet Explorer Web Folder Behaviors Cross-Domain Scripting Vulnerability
14513	Microsoft Windows Plug and Play Buffer Overflow Vulnerability
14514	Microsoft Windows Print Spooler Buffer Overflow Vulnerability
14515	Microsoft Internet Explorer Unspecified SharePoint Portal Services Log Sink ActiveX Vulnerability
14518	Microsoft Windows Telephony Service Buffer Overflow Vulnerability
14519	Microsoft Windows Kerberos Denial Of Service Vulnerability
14520	Microsoft Windows Kerberos PKINIT Man In The Middle Vulnerability

August 9, 2005 (Security Update 23.02)

This content update for Symantec ESM Network Assessment detects and reports 49 additional vulnerabilities. The following table includes information about the 49 new vulnerabilities.

Bugtraq ID	Vulnerability Name
857	Sendmail Aliases Database Regeneration Vulnerability
904	Sendmail ETRN Denial of Service Vulnerability
924	Microsoft Exchange Server AUTH / XAUTH / AUTHINFO DoS Vulnerabilities
1044	Microsoft Windows AEDEBUG Registry Key Vulnerability
1146	Sendmail mail.local Vulnerabilities
2794	Sendmail Unsafe Signal Handling Race Condition Vulnerability
2909	Microsoft IIS Unicode .asp Source Code Disclosure Vulnerability
3378	Sendmail Queue Processing Data Loss/DoS Vulnerability
3421	Microsoft Internet Explorer HTTP Request Encoding Vulnerability
3578	Microsoft Internet Explorer Arbitrary File Execution Vulnerability
3721	Microsoft IE Same Origin Policy Violation Vulnerability
3867	Microsoft Internet Explorer Arbitrary Program Execution Vulnerability
4082	Microsoft Internet Explorer Forced Script Execution Vulnerability
4752	Microsoft Internet Explorer Content-Disposition Handling File Execution Vulnerability
4753	Microsoft Internet Explorer Zone Spoofing Vulnerability
4822	Sendmail File Locking Denial Of Service Vulnerability
6535	Multiple Vendor Network Device Driver Frame Padding Information Disclosure Vulnerability
6548	Sendmail check_relay Access Bypassing Vulnerability
6991	Sendmail Header Processing Buffer Overflow Vulnerability
7230	Sendmail Address Prescan Memory Corruption Vulnerability
8234	Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability

Bugtraq ID	Vulnerability Name
8458	Microsoft RPCSS DCERPC DCOM Object Activation Packet Length Heap Corruption Vulnerability
8459	Microsoft RPCSS DCOM Interface Long Filename Heap Corruption Vulnerability
8641	Sendmail Prescan() Variant Remote Buffer Overrun Vulnerability
8649	Sendmail Ruleset Parsing Buffer Overflow Vulnerability
9105	Microsoft Outlook Express MHTML Forced File Execution Vulnerability
9107	Microsoft Outlook Express MHTML Redirection Local File Parsing Vulnerability
9182	Multiple Browser URI Display Obfuscation Weakness
9510	Microsoft Windows Shell CLSID File Extension Misrepresentation Vulnerability
9624	Microsoft Windows Internet Naming Service Buffer Overflow Vulnerability
9633	Microsoft ASN.1 Library Length Integer Mishandling Memory Corruption Vulnerability
9635	Microsoft Windows ASN.1 Library Bit String Processing Integer Handling Vulnerability
9658	Microsoft Internet Explorer ITS Protocol Zone Bypass Vulnerability
9930	Apache Error Log Escape Sequence Injection Vulnerability
10705	Microsoft Windows HTML Help Heap Overflow Vulnerability
11365	Microsoft Windows Kernel Local Denial of Service Vulnerability
14087	Microsoft Internet Explorer Javaprxy.DLL COM Object Instantiation Heap Overflow Vulnerability
14214	Microsoft Windows Color Management Module ICC Profile Buffer Overflow Vulnerability
13940	Multiple Vendor Telnet Client Remote Information Disclosure Vulnerability
13948	Microsoft Agent Trusted Content Spoofing Vulnerability
13951	Microsoft Outlook Express NNTP Response Parsing Buffer Overflow Vulnerability

Bugtraq ID	Vulnerability Name
13952	Microsoft Exchange Server Outlook Web Access HTML Injection Vulnerability
13953	Microsoft Windows HTML Help Remote Code Execution Vulnerability
13941	Microsoft Internet Explorer PNG Image Rendering Buffer Overflow Vulnerability
13943	Microsoft Internet Explorer XML Redirect Information Disclosure Vulnerability
13946	Microsoft Internet Explorer Unspecified DigWebX ActiveX Control Vulnerability
13947	Microsoft Internet Explorer Unspecified GIF And BMP Denial Of Service Vulnerability
13950	Microsoft Windows Web Client Service Remote Code Execution Vulnerability
13942	Microsoft Incoming SMB Packet Validation Remote Buffer Overflow Vulnerability

Detectable vulnerabilities and security exposures

Originally released with ESM 6.5

The following table includes a complete list of detectable vulnerabilities and security exposures for Symantec ESM Network Assessment originally released with ESM 6.5.

ID	Title
770	Alibaba Multiple CGI Vulnerabilties
115	Allaire ColdFusion Remote File Display, Deletion, Upload and Execution Vulnerability
229	Allaire Forums Getfile Vulnerability
1290	Allegro RomPager Malformed URL Request DoS Vulnerability
762	AN-HTTPd CGI Vulnerabilities
719	Anyform CGI Semicolon Vulnerability
2182	Apache /tmp File Race Vulnerability

ID	Title
5816	Apache 2 mod_dav Denial Of Service Vulnerability
6065	Apache 2 WebDAV CGI POST Request Information Disclosure Vulnerability
5486	Apache 2.0 CGI Path Disclosure Vulnerability
5434	Apache 2.0 Encoded Backslash Directory Traversal Vulnerability
5485	Apache 2.0 Path Disclosure Vulnerability
5996	Apache AB.C Web Benchmarking Buffer Overflow Vulnerability
5995	Apache AB.C Web Benchmarking Read_Connection() Buffer Overflow Vulnerability
10619	Apache ap_escape_html Memory Allocation Denial Of Service Vulnerability
7723	Apache APR_PSPrintf Memory Corruption Vulnerability
7725	Apache Basic Authentication Module Valid User Login Denial Of Service Vulnerability
5033	Apache Chunked-Encoding Memory Corruption Vulnerability
9733	Apache Cygwin Directory Traversal Vulnerability
5991	Apache HTDigest Arbitrary Command Execution Vulnerability
5990	Apache HTPasswd Insecure Temporary File Vulnerability
1284	Apache HTTP Server (win32) Root Directory Access Vulnerability
8226	Apache HTTP Server Multiple Vulnerabilities
5256	Apache httpd 2.0 CGI Error Path Disclosure Vulnerability
9829	Apache Mod_Access Access Control Rule Bypass Vulnerability
1821	Apache mod_cookies Buffer Overflow Vulnerability
9933	Apache mod_disk_cache Module Client Authentication Credential Storage Weakness
11094	Apache mod_ssl Denial Of Service Vulnerability
9826	Apache Mod_SSL HTTP Request Remote Denial Of Service Vulnerability
10736	Apache Mod_SSL Log Function Format String Vulnerability
4189	Apache mod_ssl/Apache-SSL Buffer Overflow Vulnerability

ID	Title
5787	Apache Oversized STDERR Buffer Denial Of Service Vulnerability
1728	Apache Rewrite Module Arbitrary File Disclosure Vulnerability
5847	Apache Server Side Include Cross Site Scripting Vulnerability
5054	Apache Tomcat Web Root Path Disclosure Vulnerability
5838	Apache Tomcat 3.2 Directory Disclosure Vulnerability
5542	Apache Tomcat 4.1 JSP Request Cross Site Scripting Vulnerability
2982	Apache Tomcat Cross-Site Scripting Vulnerability
5786	Apache Tomcat DefaultServlet File Disclosure Vulnerability
4877	Apache Tomcat Example Files Web Root Path Disclosure Vulnerability
6720	Apache Tomcat Example Web Application Cross Site Scripting Vulnerability
7768	Apache Tomcat Insecure Directory Permissions Vulnerability
6562	Apache Tomcat Invoker Servlet File Disclosure Vulnerability
4995	Apache Tomcat JSP Engine Denial of Service Vulnerability
6721	Apache Tomcat Null Byte Directory/File Disclosure Vulnerability
5067	Apache Tomcat Null Character Malformed Request Denial Of Service Vulnerability
4878	Apache Tomcat RealPath.JSP Malformed Request Information Disclosure Vulnerability
5193	Apache Tomcat Servlet Mapping Cross Site Scripting Vulnerability
4575	Apache Tomcat Servlet Path Disclosure Vulnerability
4876	Apache Tomcat Source.JSP Malformed Request Information Disclosure Vulnerability
4557	Apache Tomcat System Path Information Disclosure Vulnerability
6722	Apache Tomcat Web.XML File Contents Disclosure Vulnerability
11182	Apache Web Server Configuration File Environment Variable Local Buffer Overflow Vulnerability
6661	Apache Web Server Default Script Mapping Bypass Vulnerability
6939	Apache Web Server ETag Header Information Disclosure Weakness

ID	Title
7255	Apache Web Server File Descriptor Leakage Vulnerability
8135	Apache Web Server FTP Proxy IPV6 Denial Of Service Vulnerability
6660	Apache Web Server Illegal Character HTTP Request File Disclosure Vulnerability
7254	Apache Web Server Linefeed Memory Allocation Denial Of Service Vulnerability
6943	Apache Web Server MIME Boundary Information Disclosure Vulnerability
8926	Apache Web Server mod_cgid Module CGI Data Redirection Vulnerability
6659	Apache Web Server MS-DOS Device Name Arbitrary Code Execution Vulnerability
6662	Apache Web Server MS-DOS Device Name Denial Of Service Vulnerability
8911	Apache Web Server Multiple Module Local Buffer Overflow Vulnerability
7332	Apache Web Server OS2 Filestat Denial Of Service Vulnerability
8137	Apache Web Server Prefork MPM Denial Of Service Vulnerability
11187	Apache Web Server Remote IPv6 Buffer Overflow Vulnerability
5884	Apache Web Server Scoreboard Memory Segment Overwriting SIGUSR1 Sending Vulnerability
8134	Apache Web Server SSLCipherSuite Weak CipherSuite Renegotiation Weakness
8138	Apache Web Server Type-Map Recursive Loop Denial Of Service Vulnerability
2060	Apache Web Server with Php 3 File Disclosure Vulnerability
4335	Apache Win32 Batch File Remote Command Execution Vulnerability
791	Artisoft XtraMail Multiple DoS Vulnerabilities
1051	Atrium Software Mercur Mail Server 3.2 Multiple Buffer Overflows Vulnerability
716	Berkeley Sendmail Daemon Mode Vulnerability
1	Berkeley Sendmail DEBUG Vulnerability
715	Berkeley Sendmail Group Permissions Vulnerability
685	Berkeley Sendmail MIME Vulnerability

ID	Title
717	Berkeley Sendmail Starvation and Overflow Vulnerabilities
778	BigIP Config UI Vulnerabilities
1817	BNB Survey.cgi Metacharacter Vulnerability
2147	BNBForm Automessage File Retrieval Vulnerability
269	Cat Soft Serv-U Buffer Overflow Vulnerabilities
1860	CatSoft FTP Serv-U Brute-Force Vulnerability
3538	Cisco 12000 Outgoing ACL Fragmented Packet Vulnerability
3536	Cisco 12000 Series Internet Router ACL Failure To Drop Packets Vulnerability
3534	Cisco 12000 Series Internet Router Denial Of Service Vulnerability
3540	Cisco 12000 Series Turbo ACL Fragment Bypass Vulnerability
3535	Cisco Access Control List Fragment Non-blocking Vulnerability
9143	Cisco Aironet Access Point Wired Equivalent Privacy Key Disclosure Vulnerability
615	Cisco Catalyst 2900 VLAN Vulnerability
1846	Cisco Catalyst 3500 XL Remote Arbitrary Command Execution Vulnerability
2604	Cisco Catalyst 802.1x Frame Forwarding Vulnerability
7424	Cisco Catalyst CatOS Authentication Bypass Vulnerability
1122	Cisco Catalyst Enable Password Bypass Vulnerability
2072	Cisco Catalyst Memory Leak Denial of Service Vulnerability
8149	Cisco Catalyst Non-Standard TCP Flags Remote Denial Of Service Vulnerability
2689	Cisco Catalyst SNMP Empty UDP Packet Denial of Service
2117	Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability
4790	Cisco Catalyst Unicast Traffic Broadcast Vulnerability
5976	Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability
8752	Cisco CatOS Password Prompt Unauthorized Remote Command Execution Vulnerability

ID	Title
3588	Cisco Context Based Access Control Protocol Check Bypassing Vulnerability
3412	Cisco Discovery Protocol Neighbor Announcment Denial of Service Vulnerability
3539	Cisco Fragment Keyword Outgoing Access Control Vulnerability
1541	Cisco Gigabit Switch Router with Fast/Gigabit Ethernet Cards ACL Bypass/ DoS Vulnerabilities
8373	Cisco IOS 2GB HTTP GET Buffer Overflow Vulnerability
2733	Cisco IOS BGP Transitive Attribute Denial of Service Vulnerability
693	Cisco IOS CHAP Authentication Vulnerabilities
4191	Cisco IOS Cisco Express Forwarding Session Information Leakage Vulnerability
7605	Cisco IOS Crypto Engine Accelerator Access Control List Circumvention Vulnerability
6443	Cisco IOS EIGRP Announcement ARP Denial Of Service Vulnerability
315	Cisco IOS established Access List Keyword Vulnerability
1880	Cisco IOS Extended Access List Failure Vulnerability
1154	Cisco IOS HTTP %% Vulnerability
2936	Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability
10014	Cisco IOS HTTP Router Management Service Malformed Request Denial Of Service Vulnerability
4786	Cisco IOS ICMP Redirect Denial Of Service Vulnerability
6823	Cisco IOS ICMP Redirect Routing Table Modification Vulnerability
2427	Cisco IOS ILMI SNMP Community String Vulnerability
10083	Cisco IOS Malformed IKE Packet Remote Denial Of Service Vulnerability
3022	Cisco IOS Malformed PPTP Packet Denial of Service Vulnerability
8211	Cisco IOS Malicious IPV4 Packet Sequence Denial Of Service Vulnerability
9562	Cisco IOS MSFC2 Malformed Layer 2 Frame Denial Of Service Vulnerability
6895	Cisco IOS OSPF Neighbor Buffer Overflow Vulnerability

ID	Title
692	Cisco IOS Remote Router Crash
2804	Cisco IOS Router Scan Software Reloading Vulnerability
10052	Cisco IOS RST-ACK Packet Access Control Bypass Vulnerability
7607	Cisco IOS Service Assurance Agent Malformed Packet Denial Of Service Vulnerability
1838	Cisco IOS Software '?/' HTTP Request DoS Vulnerability
706	Cisco IOS Software Input Access List Leakage with NAT
1123	Cisco IOS Software TELNET Option Handling Vulnerability
675	Cisco IOS Syslog Crash
703	Cisco IOS tacacs Access List Keyword Vulnerability
5328	Cisco IOS TFTP Server Long File Name Buffer Overflow Vulnerability
3096	Cisco IOS UDP Denial of Service Vulnerability
8323	Cisco IOS UDP Echo Service Memory Disclosure Vulnerability
3547	Cisco Local Interface ARP Denial of Service Vulnerability
3537	Cisco Outbound Access Control List Bypass Vulnerability
5114	Cisco SSH Denial of Service Vulnerability
1318	Computalynx CMail Web Interface Buffer Overflow Vulnerability
128	Count.cgi (wwwcount) Buffer Overflow Vulnerability
267	Counter.exe Denial of Service Vulnerabilities
564	Dragon-Fire IDS Vulnerability
1859	Exim Buffer Overflow Vulnerability
799	FormHandler.cgi Reply Attachment Vulnerability
9954	Foxmail Remote Buffer Overflow Vulnerability
5369	Frederic Tyndiuk Eupload Plain Text Password Storage Vulnerability
2713	FreeStats.com Remote User Info Modification Vulnerability
2026	GlimpseHTTP and WebGlimpse Piped Command Vulnerability
2020	Greg Matthews Classifieds.cgi Metacharacter Vulnerability
10224	HP Web Jetadmin Multiple Vulnerabilities

ID	Title
9971	HP Web Jetadmin Printer Firmware Update Script Arbitrary File Upload Weakness
9973	HP Web Jetadmin Remote Arbitrary Command Execution Vulnerability
9972	HP Web Jetadmin setinfo.hts Script Directory Traversal Vulnerability
2056	Hylafax Faxsurvey Remote Command Execution Vulnerability
6870	IBM Lotus Domino HTTP Redirect Buffer Overflow Vulnerability
6951	IBM Lotus Domino Web Server HTTP POST Denial Of Service Vulnerability
6871	IBM Lotus Domino Web Server iNotes s_ViewName/Foldername Buffer Overflow Vulnerability
2126	iCat Carbo Server File Disclosure Vulnerability
914	IMail IMonitor status.cgi DoS Vulnerability
1995	Info2www CGI Input Handling Vulnerability
733	Internet Anywhere Mail Server DoS Vulnerability
730	Internet Anywhere Mail Server Multiple Buffer Overflow Vulnerabilities
9953	Ipswitch WS_FTP Multiple Vulnerabilities
380	IRIX cgi-bin handler Vulnerability
374	IRIX cgi-bin webdist.cgi Vulnerabilty
373	IRIX cgi-bin wrap Vulnerability
346	IRIX df Vulnerability
392	IRIX login Vulnerability
64	IRIX pfdispaly.cgi Vulnerability
2307	ISC Bind 4 nslookupComplain() Buffer Overflow Vulnerability
2309	ISC Bind 4 nslookupComplain() Format String Vulnerability
2302	ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability
4936	ISC BIND 9 Remote Denial Of Service Vulnerability
2321	ISC BIND Internal Memory Disclosure Vulnerability
2002	JJ sample CGI program Escape Character Vulnerability
3155	John O'Fallon 'responder.cgi' DoS Vulnerability

ID	Title
9975	Kerio MailServer Spam Filter Buffer Overrun Vulnerability
580	Linux Blind TCP Spoofing Vulnerability
4049	Lotus Domino Banner Information Disclosure Vulnerability
6646	Lotus Domino HTTP Authentication Logging Buffer Overflow Vulnerability
4019	Lotus Domino MS-Dos Device Name Denial Of Service Vulnerability
4406	Lotus Domino MS-DOS Device Path Disclosure Vulnerability
6128	Lotus Domino Non-existent NSF Database Banner Information Disclosure Vulnerability
4022	Lotus Domino Remote Authentication Bypass Vulnerability
3991	Lotus Domino Username Enumeration Vulnerability
4020	Lotus Domino Webserver DOS Device Extension Denial of Service Vulnerability
2080	Matt Wright FormMail Cross-Site Request Forgery Vulnerability
2079	Matt Wright FormMail Remote Command Execution Vulnerability
735	Mediahouse Statistics Server Cleartext Password Vulnerability
2674	Microsoft IIS 5.0 .printer ISAPI Extension Buffer Overflow Vulnerability
6214	Microsoft Data Access Components RDS Buffer Overflow Vulnerability
728	Microsoft Excel File Import Macro Execution Vulnerability
4053	Microsoft Exchange Inappropriate Registry Permissions Vulnerability
8838	Microsoft Exchange Server Buffer Overflow Vulnerability
1205	Microsoft FrontPage Extensions .pwd File Permissions Vulnerability
5804	Microsoft FrontPage Server Extensions SmartHTML Buffer Overflow Vulnerability
598	Microsoft IE5 ActiveX 'Object for constructing type libraries for scriptlets' Vulnerability
619	Microsoft IE5 ActiveX 'Eyedog' Vulnerability
828	Microsoft IE5 Offline Browsing Pack Task Scheduler Vulnerability
1818	Microsoft IIS 3.0 newdsn.exe File Creation Vulnerability

ID	Title
1565	Microsoft IIS 4.0/5.0 File Permission Canonicalization Vulnerability
1191	Microsoft IIS 4.0/5.0 Malformed .htr Request Vulnerability
1193	Microsoft IIS 4.0/5.0 Malformed Filename Request Vulnerability
1578	Microsoft IIS 5.0 'Translate: f' Source Disclosure Vulnerability
1806	Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability
4478	Microsoft IIS ASP Server-Side Include Buffer Overflow Vulnerability
4490	Microsoft IIS Chunked Encoding Heap Overflow Variant Vulnerability
4485	Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability
4525	Microsoft IIS CodeBrws.ASP Source Code Disclosure Vulnerability
1912	Microsoft IIS Executable File Parsing Vulnerability
4482	Microsoft IIS FTP Connection Status Request Denial of Service Vulnerability
4855	Microsoft IIS HTR Chunked Encoding Transfer Heap Overflow Vulnerability
4474	Microsoft IIS HTR ISAPI Extension Buffer Overflow Vulnerability
4476	Microsoft IIS HTTP Header Field Delimiter Buffer Overflow Vulnerability
2654	Microsoft IIS Long URL Denial of Service Vulnerability
1081	Microsoft IIS UNC Mapped Virtual Host Vulnerability
6070	Microsoft IIS WebDAV Denial Of Service Vulnerability
2690	Microsoft IIS WebDAV 'Propfind' Server Restart Vulnerability
9109	Microsoft Internet Explorer BackToFramedJPU Cross-Domain Policy Vulnerability
9663	Microsoft Internet Explorer Bitmap Processing Integer Overflow Vulnerability
8454	Microsoft Internet Explorer BR549.DLL ActiveX Control Buffer Overflow Vulnerability
8556	Microsoft Internet Explorer Browser Popup Window Object Type Validation Vulnerability
11377	Microsoft Internet Explorer Double Byte Character Set Handling Address Bar Spoofing Vulnerability

ID	Title
9629	Microsoft Internet Explorer Double-Null URI Denial Of Service Vulnerability
9015	Microsoft Internet Explorer ExecCommand Cross-Domain Access Violation Vulnerability
9278	Microsoft Internet Explorer File Download Warning Bypass Vulnerability
9014	Microsoft Internet Explorer Function Pointer Override Cross-Domain Access Violation Vulnerability
11367	Microsoft Internet Explorer Heartbeat ActiveX Control Unspecified Vulnerability
10973	Microsoft Internet Explorer Implicit Drag and Drop File Installation Vulnerability
11366	Microsoft Internet Explorer Install Engine ActiveX Control Buffer Overflow Vulnerability
9106	Microsoft Internet Explorer Invalid ContentType Cache Directory Location Disclosure Weakness
10689	Microsoft Internet Explorer JavaScript Method Assignment Cross-Domain Scripting Vulnerability
8530	Microsoft Internet Explorer Malformed GIF Double Free Code Execution Vulnerability
9108	Microsoft Internet Explorer Method Caching Mouse Click Event Hijacking Vulnerability
10473	Microsoft Internet Explorer Modal Dialog Zone Bypass Vulnerability
9009	Microsoft Internet Explorer Mouse Click Event Hijacking Vulnerability
9568	Microsoft Internet Explorer NavigateAndFind() Cross-Zone Policy Vulnerability
7806	Microsoft Internet Explorer OBJECT Tag Buffer Overflow Vulnerability
8456	Microsoft Internet Explorer Object Type Validation Vulnerability
11381	Microsoft Internet Explorer Plug-in Navigations Handling Address Bar Spoofing Vulnerability
10690	Microsoft Internet Explorer Popup.show Mouse Event Hijacking Vulnerability
9013	Microsoft Internet Explorer Script URL Cross-Domain Access Violation Vulnerability

ID	Title
11383	Microsoft Internet Explorer Secure Sockets Layer Caching Vulnerability
9628	Microsoft Internet Explorer Shell: IFrame Cross-Zone Scripting Vulnerability
10816	Microsoft Internet Explorer Style Tag Comment Memory Corruption Vulnerability
11388	Microsoft Internet Explorer Unspecified showHelp Zone Bypass Vulnerability
9769	Microsoft Internet Explorer window.open Media Bar Cross-Zone Scripting Vulnerability
9798	Microsoft Internet Explorer window.open Search Pane Cross-Zone Scripting Vulnerability
9012	Microsoft Internet Explorer XML Object Zone Restriction Bypass Vulnerability
8565	Microsoft Internet Explorer XML Page Object Type Validation Vulnerability
8457	Microsoft Internet Explorer Zone Restriction Bypass Script Execution Vulnerability
3420	Microsoft Internet Explorer Zone Spoofing Vulnerability
9828	Microsoft MSN Messenger Information Disclosure Vulnerability
1197	Microsoft Office 2000 UA Control Vulnerability
10711	Microsoft Outlook Express Malformed Email Header Denial Of Service Vulnerability
3104	Microsoft Remote Procedure Call Service DoS Vulnerability
5014	Microsoft SQL Server 2000 Password Encrypt Procedure Buffer Overflow Vulnerability
5310	Microsoft SQL Server 2000 Resolution Service Heap Overflow Vulnerability
5311	Microsoft SQL Server 2000 Resolution Service Stack Overflow Vulnerability
4231	Microsoft SQL Server Multiple Extended Stored Procedure Buffer Overflow Vulnerabilities
4135	Microsoft SQL Server OLE DB Provider Name Buffer Overflow Vulnerability

ID	Title
5004	Microsoft SQL Server SQLXML Buffer Overflow Vulnerability
5005	Microsoft SQL Server SQLXML Script Injection Vulnerability
5411	Microsoft SQL Server User Authentication Remote Buffer Overflow Vulnerability
3499	Microsoft UPnP Denial of Service Vulnerability
11378	Microsoft Window Management API Local Privilege Escalation Vulnerability
2394	Microsoft Windows 2000 Domain Controller DoS Vulnerability
2988	Microsoft Windows 2000 SMTP Improper Authentication Vulnerability
10123	Microsoft Windows COM Internet Service/RPC Over HTTP Remote Denial Of Service Vulnerability
8205	Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability
10119	Microsoft Windows Help And Support Center URI Validation Code Execution Vulnerability
11369	Microsoft Windows Kernel Virtual DOS Machine Privilege Escalation Vulnerability
6666	Microsoft Windows Locator Service Buffer Overflow Vulnerability
10108	Microsoft Windows LSASS Buffer Overrun Vulnerability
7640	Microsoft Windows Media Player Automatic File Download and Execution Vulnerability
8263	Microsoft Windows Media Player IE Zone Access Control Bypass Vulnerability
8826	Microsoft Windows Messenger Service Buffer Overrun Vulnerability
11372	Microsoft Windows NetDDE Remote Buffer Overflow Vulnerability
4236	Microsoft Windows NT Security Policy Bypass Vulnerability
2244	Microsoft Windows NT SNMP-WINS DoS Vulnerability
7116	Microsoft Windows ntdll.dll Buffer Overflow Vulnerability
10121	Microsoft Windows Object Identity Network Communication Vulnerability
10677	Microsoft Windows Program Group Converter Filename Local Buffer Overrun Vulnerability
6830	Microsoft Windows Remote Registry Modification Weakness

ID	Title
6005	Microsoft Windows RPC Service Denial of Service Vulnerability
8811	Microsoft Windows RPCSS Multi-thread Race Condition Vulnerability
10127	Microsoft Windows RPCSS Service Remote Denial Of Service Vulnerability
10213	Microsoft Windows Shell Long Share Name Buffer Overrun Vulnerability
10708	Microsoft Windows Task Scheduler Remote Buffer Overflow Vulnerability
11375	Microsoft Windows WMF/EMF Image Format Rendering Remote Buffer Overflow Vulnerability
9892	Microsoft Windows XP explorer.exe Remote Denial of Service Vulnerability
898	Mini-SQL w3-msql Buffer Overflow Vulnerabilities
2001	Miva htmlscript 2.x Directory Traversal Vulnerability
5084	Mod_SSL Off-By-One HTAccess Buffer Overflow Vulnerability
6029	Mod_SSL Wildcard DNS Cross Site Scripting Vulnerability
2708	MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability
1084	MS Index Server '%20' ASP Source Disclosure Vulnerability
5981	Multiple Apache HTDigest and HTPassWD Component Vulnerabilites
5993	Multiple Apache HTDigest Buffer Overflow Vulnerabilities
9182	Multiple Browser URI Display Obfuscation Weakness
2247	Multiple Linux Vendor Zero-Length Fragment Vulnerability
8577	Multiple Microsoft Internet Explorer Script Execution Vulnerabilities
2010	Multiple Vendor 'Out Of Band' Data Denial Of Service Vulnerability
788	Multiple Vendor BIND (NXT Overflow & Denial of Service) Vulnerabilities
1923	Multiple Vendor BIND 8.2.2-P5 Denial of Service Vulnerability
134	Multiple Vendor BIND iquery buffer overflow Vulnerability
2242	Multiple Vendor FTP Long Path Buffer Overflow Vulnerability
113	Multiple Vendor FTPD realpath Vulnerability
1425	Multiple Vendor ftpd setproctitle() Format String Vulnerability
4131	Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability

ID	Title
687	Multiple Vendor INN remote Vulnerability
9841	Multiple Vendor Internet Browser Cookie Path Argument Restriction Bypass Vulnerability
121	Multiple Vendor Linux Mountd Vulnerability
2666	Multiple Vendor loopback (land.c) Denial of Service Vulnerability
1760	Multiple Vendor MIME Header DoS Vulnerability
711	Multiple Vendor Natural Language Service (NLS) Vulnerability
686	Multiple Vendor nph-test-cgi Vulnerability
6904	Multiple Vendor Session Initiation Protocol Vulnerabilities
6407	Multiple Vendor SSH2 Implementation Buffer Overflow Vulnerabilities
127	Multiple Vendor Statd Buffer Overflow Vulnerability
3064	Multiple Vendor Telnetd Buffer Overflow Vulnerability
2003	Multiple Vendor test-cgi Directory Listing Vulnerability
122	Multiple Vendor ToolTalk RPC Service Overflow Vulnerability
599	Multiple Vendor Wu-Ftpd Buffer Overflow Vulnerability
1826	MySQL Authentication Algorithm Vulnerability
5511	MySQL Bind Address Not Enabled Weak Default Configuration Vulnerability
6373	MySQL COM_CHANGE_USER Password Length Account Compromise Vulnerability
6375	MySQL COM_CHANGE_USER Password Memory Corruption Vulnerability
6368	MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
5853	MySQL DataDir Parameter Local Buffer Overflow Vulnerability
6718	MySQL Double Free Heap Corruption Vulnerability
926	MySQL GRANT Global Password Changing Vulnerability
7887	MySQL libmysqlclient Library mysql_real_connect() Buffer Overrun Vulnerability
6374	MySQL libmysqlclient Library Read_One_Row Buffer Overflow Vulnerability

ID	Title
6370	MySQL libmysqlclient Library Read_Rows Buffer Overflow Vulnerability
2262	Mysql Local Buffer Overflow Vulnerability
5513	MySQL Logging Not Enabled Weak Default Configuration Vulnerability
8796	MySQL Multiple Vulnerabilities
10981	MySQL Mysql_real_connect Function Potential Remote Buffer Overflow Vulnerability
7052	MySQL mysqld Privilege Escalation Vulnerability
5503	MySQL Null Root Password Weak Default Configuration Vulnerability
8590	MySQL Password Handler Buffer Overflow Vulnerability
2522	MySQL Root Operation Symbolic Link File Overwriting Vulnerability
2380	MySQL SHOW GRANTS Pasword Hash Disclosure Vulnerability
975	MySQL Unauthenticated Remote Access Vulnerability
7500	MySQL Weak Password Encryption Vulnerability
3158	NCSA HTTPd Buffer Overflow Vulnerability
1975	NCSA HTTPd campas sample script Vulnerability
4024	Netgear RT314/RT311 Gateway Router Cross-Site Scripting Vulnerability
819	NetTerm FTP Server Multiple Vulnerabilities
528	Netware IPX Admin Session Spoof Vulnerability
2025	Novell NetWare Web Server 2.x convert.bas Vulnerability
2076	Novell Netware Web Server 3.x files.pl Vulnerability
567	NT Exchange Server Encapsulated SMTP Address Vulnerability
529	NT IIS MDAC RDS Vulnerability
167	NT IIS Showcode ASP Vulnerability
950	NT Index Server Directory Traversal Vulnerability
1264	NT Login Request Size Mismatch DoS Vulnerability
959	NT LsaQueryInformationPolicy() Domain SID Leak Vulnerability
2540	Ntpd Remote Buffer Overflow Vulnerability
1808	OmniHTTPD visiadmin.exe Denial of Service Vulnerability

ID	Title
8628	OpenSSH Buffer Mismanagement Vulnerabilities
3614	OpenSSH UseLogin Environment Variable Passing Vulnerability
5364	OpenSSL ASCII Representation Of Integers Buffer Overflow Vulnerability
5366	OpenSSL ASN.1 Parsing Error Denial Of Service Vulnerability
8732	OpenSSL ASN.1 Parsing Vulnerabilities
7148	OpenSSL Bad Version Oracle Side Channel Attack Vulnerability
6884	OpenSSL CBC Error Information Leakage Weakness
9899	OpenSSL Denial of Service Vulnerabilities
5361	OpenSSL Kerberos Enabled SSLv3 Master Key Exchange Buffer Overflow Vulnerability
3004	OpenSSL PRNG Internal State Disclosure Vulnerability
5363	OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability
5362	OpenSSL SSLv3 Session ID Buffer Overflow Vulnerability
7101	OpenSSL Timing Attack RSA Private Key Information Disclosure Vulnerability
3187	OpenSSL Unseeded Random Number Generator Vulnerability
161	OpenVMS loginout Vulnerability
6849	Oracle Database Server ORACLE.EXE Buffer Overflow Vulnerability
4033	Oracle TNS Listener Arbitrary Library Call Execution Vulnerability
2078	OReilly WebSite 1.x/2.0 win-c-sample.exe Buffer Overflow Vulnerability
1611	O'Reilly WebSite Pro Write Access Vulnerability
629	phf Remote Command Execution Vulnerability
6557	PHP 4.0.3 IMAP Module Buffer Overflow Vulnerability
7256	PHP array_pad() Integer Overflow Memory Corruption Vulnerability
6875	PHP CGI SAPI Code Execution Vulnerability
7199	PHP emalloc() Unspecified Integer Overflow Memory Corruption Vulnerability
5278	PHP HTTP POST Incorrect MIME Header Parsing Vulnerability

ID	Title
5562	PHP Mail Function ASCII Control Character Header Spoofing Vulnerability
10725	PHP memory_limit Remote Code Execution Vulnerability
4026	PHP MySQL Safe_Mode Filesystem Circumvention Vulnerability
7210	PHP openlog() Buffer Overflow Vulnerability
7805	PHP PHPInfo Cross-Site Scripting Vulnerability
4183	PHP Post File Upload Buffer Overflow Vulnerabilities
2954	PHP SafeMode Arbitrary File Execution Vulnerability
7187	PHP socket_iovec_alloc() Integer Overflow Vulnerability
7197	PHP socket_recv() Signed Integer Memory Corruption Vulnerability
7198	PHP socket_recvfrom() Signed Integer Memory Corruption Vulnerability
7259	PHP STR_Repeat Boundary Condition Error Vulnerability
10724	PHP Strip_Tags() Function Bypass Vulnerability
7761	PHP Transparent Session ID Cross Site Scripting Vulnerability
1649	PHP Upload Arbitrary File Disclosure Vulnerability
6488	PHP wordwrap() Heap Corruption Vulnerability
712	PHP/FI Buffer Overflow Vulnerability
9782	ProFTPD _xlate_ascii_write() Buffer Overrun Vulnerability
133	Qualcomm POP Server Buffer Overflow Vulnerability
7294	Samba 'call_trans2open' Remote Buffer Overflow Vulnerability
10781	Samba Filename Mangling Method Buffer Overrun Vulnerability
5587	Samba Improperly Terminated Struct Buffer Overflow Vulnerability
2617	Samba Insecure TMP file Symbolic Link Vulnerability
1816	SAMBA Long Password Buffer Overflow Vulnerability
7295	Samba Multiple Unspecified Remote Buffer Overflow Vulnerabilities
7107	Samba REG File Writing Race Condition Vulnerability
2928	Samba Remote Arbitrary File Creation Vulnerability
6210	Samba Server Encrypted Password Buffer Overrun Vulnerability

ID	Title
7106	Samba SMB/CIFS Packet Assembling Buffer Overflow Vulnerability
1874	SAMBA SWAT Logfile Permissions Vulnerability
1873	SAMBA SWAT Logging Failure Vulnerability
1872	SAMBA SWAT Symlink Vulnerability
10780	Samba Web Administration Tool Base64 Decoder Buffer Overflow Vulnerability
7206	Samba-TNG Unspecified Remote Privilege Escalation Vulnerability
1663	SCO Unixware '/search97cgi/vtopic' Vulnerability
3163	Sendmail Debugger Arbitrary Code Execution Vulnerability
5122	Sendmail DNS Map TXT Record Buffer Overflow Vulnerability
8485	Sendmail DNS Maps Remote Denial of Service Vulnerability
8674	Sendmail Headers Prescan Denial Of Service Vulnerability
3377	Sendmail Inadequate Privilege Lowering Vulnerability
2308	Sendmail Invalid MAIL/RCPT Vulnerability
5770	Sendmail Long Ident Logging Circumvention Weakness
5845	Sendmail SMRSH Double Pipe Access Validation Vulnerability
5921	Sendmail Trojan Horse Vulnerability
7829	Sendmail V.5 -oR Privilege Escalation Vulnerability
2052	Serv-U FTP Directory Traversal Vulnerability
1016	Serv-U FTP Server Path Disclosure Vulnerability
859	Serv-U FTP Server SITE PASS DoS Vulnerability
2251	Skunkware view-source Directory Traversal Vulnerability
153	SLMail 3.0.2421 Buffer Overflow 'Mail From' Vulnerability
2558	Solaris 7/8 kcms_configure Command-Line Buffer Overflow Vulnerability
4674	Solaris cachefsd Heap Overflow Vulnerability
205	Solaris rpcbind Listening on a Non-Standard Port Vulnerability
866	Solaris sadmind Buffer Overflow Vulnerability
921	SolutionScripts Home Free search.cgi Directory Traversal Vulnerability

ID	Title
2347	SSH CRC-32 Compensation Attack Detector Vulnerability
138	ssh-agent Vulnerability
1623	Stalkerlab's Mailers 1.1.2 CGI Mail Spoofing Vulnerability
9962	Sun Solaris vfs_getvfssw function Local Privilege Escalation Vulnerability
428	SunOS rpc.cmsd Vulnerability
1656	SuSE Apache WebDAV Directory Listings Vulnerability
2276	Sysadmin Magazine man.sh Arbitrary Command Execution Vulnerability
2265	textcounter.pl Arbitrary Command Execution Vulnerability
961	Tiny FTPd Multiple Buffer Overflow Vulnerabilities
2024	Webcom Datakommunikation CGI Guestbook rguest/wguest Vulnerability
2058	WEBgais Remote Command Execution Vulnerability
2077	WEBgais websendmail Remote Command Execution Vulnerability
5048	WebScripts WebBBS Remote Command Execution Vulnerability
892	WebWho+ Remote Command Execution Vulnerability
747	WFTPD Remote Buffer Overflow Vulnerability
217	WS_FTP Server Denial of Service Vulnerability
2241	wu-ftpd /bin SITE EXEC Misconfiguration Vulnerability
2296	Wu-Ftpd Debug Mode Client Hostname Format String Vulnerability
1387	Wu-Ftpd Remote Format String Stack Overwrite Vulnerability
9832	WU-FTPD restricted-gid Unauthorized Access Vulnerability
737	Wu-ftpd SITE NEWER Denial of Service Vulnerability
649	WWWBoard Password Disclosure Vulnerability
2317	www-sql .htaccess bypass Vulnerability