

Symantec Vulnerability Assessment Vulnerability Updates Release Notes



Symantec Vulnerability Assessment Vulnerability Updates Release Notes

The software that is described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 2007 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks, and LiveUpdate, Symantec NetRecon, Symantec Enterprise Security Architecture, Symantec Enterprise Security Manager, and Symantec Security Response are trademarks of Symantec Corporation.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks and Windows Server 2003 is a trademark of Microsoft Corporation.

Other product names that are mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

Technical support

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

Symantec technical support offerings include:

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

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

Licensing and registration

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

Contacting Technical Support

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

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.

Vulnerability Update Release Notes

March 2, 2007	13
January 30, 2007	15
December 29, 2006	15
October 19, 2006	16
September 21, 2006	18
August 18, 2006	19
July 18, 2006	22
June 21, 2006	24
May 30, 2006	26
May 10, 2006	26
April 19, 2006	27
March 28, 2006	28
March 16, 2006	29
February 28, 2006	30
February 15, 2006	30
February 8, 2006	31
January 25, 2006	32
January 11, 2006	32
January 4, 2006	33
December 20, 2005	33
December 13, 2005	34
December 7, 2005	35
November 22, 2005	35
November 8, 2005	36
October 25, 2005	37
October 11, 2005	37
September 27, 2005	38
September 14, 2005	40
August 30, 2005	40
August 23, 2005	41
August 11, 2005	41
July 21, 2005	42
July 13, 2005	43
June 28, 2005	44
June 15, 2005	46
June 7, 2005	47
May 24, 2005	48
May 11, 2005	49
April 26, 2005	50
April 14, 2005	51

March 31, 2005	53
March 23, 2005	54
March 8, 2005	55
February 22, 2005	56
February 10, 2005	57
January 25, 2005	59
January 12, 2005	59
January 10, 2005	60
December 22, 2004	60
December 15, 2004	61
December 2, 2004	63
November 30, 2004	63
November 16, 2004	64
November 9, 2004	65
November 2, 2004	65
October 18, 2004	67
October 12, 2004	68
October 6, 2004	69
September 21, 2004	70
September 14, 2004	71
September 7, 2004	71
August 18, 2004	72
August 10, 2004	74
July 30, 2004	75
July 27, 2004	75
July 13, 2004	79
July 6, 2004	80
June 29, 2004	81
June 15, 2004	83
June 8, 2004	84
June 1, 2004	84
May 18, 2004	85
May 11, 2004	86
May 4, 2004	86
April 20, 2004	88
April 13, 2004	89
April 6, 2004	90
March 23, 2004	92
March 9, 2004	94
February 24, 2004	96
February 10, 2004	97
February 3, 2004	98
January 27, 2004	98

January 14, 2004	99
December 30, 2003	100
December 17, 2003	101
December 3, 2003	103
November 20, 2003	104
November 11, 2003	106
November 6, 2003	106
October 23, 2003	109
October 15, 2003	111
October 8, 2003	111
September 24, 2003	112
September 16, 2003	112
September 11, 2003	113
August 28, 2003	113
August 12, 2003	115
July 29, 2003	117
July 17, 2003	117
July 15, 2003	118

Vulnerability Update Release Notes

March 2, 2007

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 22 additional vulnerabilities and 1 updated vulnerability. The following table includes information about the 22 additional vulnerabilities.

Bugtraq ID	Title
22478	Microsoft HTML Help ActiveX Control Remote Code Execution Vulnerability
20704	Microsoft Internet Explorer ADODB.Connection Execute Memory Corruption Vulnerability
21451	Microsoft Word Malformed String Arbitrary Remote Code Execution Vulnerability
21518	Microsoft Word Malformed Data Structures Code Execution Vulnerability
21589	Microsoft Word Code Execution Vulnerability
22225	Microsoft Word 2000 Malformed Function Code Execution Vulnerability
22482	Microsoft Word Malformed Drawing Object Arbitrary Code Execution Vulnerability
22477	Microsoft Word Macro Permissions Bypass Arbitrary Code Execution Vulnerability
20325	Microsoft PowerPoint Record Improper Memory Access Remote Code Execution Vulnerability
22383	Microsoft Office Malformed String Remote Code Execution Vulnerability

Bugtraq ID	Title
22486	Microsoft Internet Explorer IMJPCSI 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
21876	Microsoft Office And Microsoft Windows RichEdit Component Remote Code Execution Vulnerability
21856	Microsoft Excel IMDATA Record Remote Code Execution Vulnerability
21877	Microsoft Excel Malformed String Remote Code Execution Vulnerability
21922	Microsoft Excel Malformed Palette Record Remote Code Execution Vulnerability
21925	Microsoft Excel Malformed Column Record Remote Code Execution Vulnerability

The following table includes information about the 1 updated vulnerability.

Bugtraq ID	Title
21952	Microsoft Excel Opcode Handling Unspecified Remote Code Execution Vulnerability

January 30, 2007

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 5 additional vulnerabilities. The following table includes information about the 5 additional vulnerabilities.

Bugtraq ID	Title
21952	Microsoft Excel Opcode Handling Unspecified Remote Code Execution Vulnerability
21931	Microsoft Outlook VEVENT Record Remote Code Execution Vulnerability
21936	Microsoft Outlook Advanced Find Remote Code Execution Vulnerability
21937	Microsoft Outlook Malformed Email Header Remote Denial of Service Vulnerability
21930	Microsoft Windows Vector Markup Language Buffer Overrun Vulnerability

December 29, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 20 additional vulnerabilities. The following table includes information about the 20 additional vulnerabilities.

Bugtraq ID	Title
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

Bugtraq ID	Title
21501	Microsoft Outlook Express Windows Address Book Contact Record Remote Code Execution Vulnerability
21495	Microsoft Windows 2000 Remote Installation Service Remote Code Execution Vulnerability
19738	Microsoft Internet Explorer Daxctle.OCX Spline Method Heap Buffer Overflow Vulnerability
20047	Microsoft Internet Explorer Daxctle.OCX KeyFrame Method Heap Buffer Overflow Vulnerability
20915	Microsoft XML Core Service XMLHTTP ActiveX Control Remote Code Execution
21020	Microsoft Internet Explorer HTML Rendering Remote Code Execution Vulnerability
21034	Microsoft Agent ActiveX Control Remote Code Execution Vulnerability
20985	Microsoft Windows Workstation Service NetpManageIPCCconnect 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 19, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 25 additional vulnerabilities. The following table includes information about the 25 additional vulnerabilities.

Bugtraq ID	Title
19030	Microsoft WebViewFolderIcon ActiveX Control Buffer Overflow Vulnerability
20226	Microsoft PowerPoint Unspecified Remote Code Execution Vulnerability
20304	Microsoft PowerPoint Object Pointer Remote Code Execution Vulnerability

Bugtraq ID	Title
20322	Microsoft PowerPoint Data Record Remote Code Execution Vulnerability
20325	Microsoft PowerPoint Record Improper Memory Access Remote Code Execution Vulnerability
20344	Microsoft Excel DATETIME Remote Code Execution Vulnerability
20338	Microsoft Windows XML Core Services XSLT Buffer Overrun Vulnerability
20382	Microsoft Office Improper Memory Access Remote Code Execution Vulnerability
20383	Microsoft Office Malformed Chart Record Remote Code Execution Vulnerability
20384	Microsoft Office Malformed Record Remote Code Execution Vulnerability
20320	Microsoft Office Smart Tag Remote Code Execution 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
20096	Microsoft Internet Explorer Vector Markup Language Buffer Overflow Vulnerability
20318	Microsoft Windows Object Packager Remote Code Execution Vulnerability
19215	Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability
20373	Microsoft Windows SMB Rename Remote Denial of Service Vulnerability
18872	Microsoft Excel Style Handling and Repair Remote Code Execution Vulnerability
20345	Microsoft Excel Lotus 1-2-3 File Handling Remote Code Execution Vulnerability
20391	Microsoft Excel COLINFO Remote Code Execution Vulnerability
19835	Microsoft Word Malformed Stack Remote Code Execution Vulnerability
20358	Microsoft Word Mail Merge Remote Code Execution Vulnerability
20341	Microsoft Word Malformed String Remote Code Execution Vulnerability
20339	Microsoft XML Core Services Information Disclosure Vulnerability

September 21, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 30 additional vulnerabilities. The following table includes information about the 30 additional vulnerabilities.

Bugtraq ID	Title
19535	HP-UX LP Subsystem Denial of Service Vulnerability
19528	HP-UX Trusted Mode Unspecified Local Denial of Service Vulnerability
19786	IBM AIX Dterm Local Privilege Escalation Vulnerability
19927	Microsoft Indexing Service Query Validation Cross-Site Scripting Vulnerability
19529	Microsoft Internet Explorer CHTSKDIC.DLL Denial Of Service Vulnerability
19667	Microsoft Internet Explorer HTTP 1.1 and Compression Long URI Buffer Overflow Vulnerability
19364	Microsoft Internet Explorer IFrame Refresh Denial of Service Vulnerability
19521	Microsoft Internet Explorer IMSKDIC.DLL Denial Of Service Vulnerability
19530	Microsoft Internet Explorer MSOE.DLL Denial Of Service Vulnerability
19640	Microsoft Internet Explorer Multiple COM Object Color Property Denial of Service Vulnerabilities
19570	Microsoft Internet Explorer TSUserEX.DLL ActiveX Control Memory Corruption Vulnerability
19572	Microsoft Internet Explorer Visual Studio COM Object Instantiation Denial of Service Vulnerability
19922	Microsoft PGM Remote Buffer Overflow Vulnerability
19229	Microsoft PowerPoint Unspecified Code Execution Vulnerability
19951	Microsoft Publisher Font Parsing Remote Code Execution Vulnerability
19636	Microsoft Windows 2000 Multiple COM Object Instantiation Code Execution Vulnerabilities
19389	Microsoft Windows Explorer Drag and Drop Remote Code Execution Vulnerability
19365	Microsoft Windows GDI32.DLL WMF Remote Denial of Service Vulnerability

Bugtraq ID	Title
19520	Microsoft Windows PNG File IHDR Block Denial of Service Vulnerability
19384	Microsoft Windows Unhandled Exception Remote Code Execution Vulnerability
19375	Microsoft Windows User Profile Privilege Escalation Vulnerability
19678	Mozilla Firefox FTP Denial of Service Vulnerability
19488	Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability
19534	Mozilla Firefox XML Handler Race Condition Memory Corruption Vulnerability
19491	Opera Web Browser IRC Chat Client Remote Denial of Service Vulnerability
19643	Sun Solaris File System Management RBAC Profile Arbitrary Command Execution Vulnerability
19657	Sun Solaris Format(1M) Buffer Overflow Vulnerability
19647	Sun Solaris Format(1M) Local Privilege Escalation Vulnerability
19662	Sun Solaris UCB/PS Command Local Information Disclosure Vulnerability
19353	Yahoo! Messenger File Extension Spoofing Vulnerability

August 18, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 56 additional vulnerabilities. The following table includes information about the 56 additional vulnerabilities.

Bugtraq ID	Title
18974	LibICE Unspecified Denial of Service Vulnerability
18872	Microsoft Excel Style Handling and Repair Remote Code Execution Vulnerability
18500	Microsoft HLINK.DLL Link Memory Corruption Vulnerability
19405	Microsoft Hyperlink Object Library Function Remote Buffer Overflow Vulnerability
18900	Microsoft Internet Explorer 6 RDS.DataControl Denial Of Service Vulnerability

Bugtraq ID	Title
19227	Microsoft Internet Explorer ADODB.Recordset NextRecordset Denial of Service Vulnerability
19316	Microsoft Internet Explorer Chained Cascading Style Sheets Remote Code Execution Vulnerability
19340	Microsoft Internet Explorer COM Object Instantiation Code Execution Vulnerability
19092	Microsoft Internet Explorer Content-Type Denial Of Service Vulnerability
19069	Microsoft Internet Explorer DataSourceControl Denial of Service Vulnerability
19228	Microsoft Internet Explorer Deleted Frame Object Denial Of Service Vulnerability
18902	Microsoft Internet Explorer DirectAnimation.DAUserData Denial Of Service Vulnerability
19204	Microsoft Internet Explorer DXImageTransform Properties Denial Of Service Vulnerability
18277	Microsoft Internet Explorer Frameset Memory Corruption Vulnerability
11826	Microsoft Internet Explorer FTP URI Arbitrary FTP Server Command Execution Vulnerability
19312	Microsoft Internet Explorer HTML Layout and Positioning Remote Code Execution Vulnerability
18929	Microsoft Internet Explorer HtmlDlgSafeHelper Remote Denial Of Service Vulnerability
19109	Microsoft Internet Explorer Internet.HHCtrl Click Denial Of Service Vulnerability
19013	Microsoft Internet Explorer MHTMLFile Denial Of Service Vulnerability
19113	Microsoft Internet Explorer Multiple Object ListWidth Property Denial Of Service Vulnerability
19140	Microsoft Internet Explorer Native Function Iterator Denial Of Service Vulnerability
19184	Microsoft Internet Explorer NDFXArtEffects Stack Overflow Vulnerability
19114	Microsoft Internet Explorer NMSA.ASFSourceMediaDescription Stack Overflow Vulnerability

Bugtraq ID	Title
18903	Microsoft Internet Explorer Object.Microsoft.DXTFilter Denial Of Service Vulnerability
18682	Microsoft Internet Explorer OuterHTML Redirection Handling Information Disclosure Vulnerability
19079	Microsoft Internet Explorer OVCl Denial Of Service Vulnerability
18960	Microsoft Internet Explorer RevealTrans Denial Of Service Vulnerability
19400	Microsoft Internet Explorer Source Element Cross-Domain Information Disclosure Vulnerability
19102	Microsoft Internet Explorer String To Binary Function Denial Of Service Vulnerability
18855	Microsoft Internet Explorer Structured Graphics Control Denial Of Service Vulnerability
18873	Microsoft Internet Explorer Table Frameset Denial Of Service Vulnerability
18946	Microsoft Internet Explorer TriEditDocument Denial Of Service Vulnerability
19030	Microsoft Internet Explorer WebViewFolderIcon Denial Of Service Vulnerability
19339	Microsoft Internet Explorer Window Location Cross-Domain Information Disclosure Vulnerability
19417	Microsoft Management Console Zone Bypass Vulnerability
18905	Microsoft Office MSO.DLL LsCreateLine() Potential Code Execution Vulnerability
18993	Microsoft Powerpoint Multiple Unspecified Vulnerabilities
18957	Microsoft Powerpoint Remote Code Execution Vulnerability
19341	Microsoft Powerpoint Remote Code Execution Vulnerability
19414	Microsoft Visual Basic for Applications Document Check Buffer Overflow Vulnerability
19388	Microsoft Windows 2000 Kernel Local Privilege Escalation Vulnerability
19404	Microsoft Windows DNS Client Buffer Overrun Vulnerability
19221	Microsoft Windows Graphical Device Interface Plus Library Denial Of Service Vulnerability

Bugtraq ID	Title
18769	Microsoft Windows HTML Help HHCtrl ActiveX Control Memory Corruption Vulnerability
18198	Microsoft Windows MHTML URI Buffer Overflow Vulnerability
19135	Microsoft Windows Remote Denial of Service Vulnerability
19300	Microsoft Windows Routing and Remote Access Denial of Service Vulnerability
19409	Microsoft Windows Server Service Remote Buffer Overflow Vulnerability
19215	Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability
19319	Microsoft Winsock Gethostbyname Buffer Overflow Vulnerability
19192	Mozilla Firefox Javascript Navigator Object Remote Code Execution Vulnerability
19197	Mozilla Foundation Products XPCOM Memory Corruption Vulnerability
19181	Mozilla Multiple Products Remote Vulnerabilities
19166	Opera Web Browser CSS Background HTTPS URI Memory Corruption Vulnerability
18972	Sun Solaris NIS Server YPServ Unspecified Denial of Service Vulnerability
19211	Yahoo! Messenger Remote Search String Arbitrary Browser Navigation Vulnerability

July 18, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 35 additional vulnerabilities. The following table includes information about the 35 additional vulnerabilities.

Bugtraq ID	Title
18603	HP-UX Kernel Unspecified Local Denial of Service Vulnerability
18748	HP-UX Mkdir Local Unauthorized Access Vulnerability
18457	HP-UX Support Tools Manager Unspecified Local Denial of Service Vulnerability
18888	Microsoft Excel COLINFO Record Remote Code Execution Vulnerability
18938	Microsoft Excel File Rebuilding Remote Code Execution Vulnerability

Bugtraq ID	Title
18890	Microsoft Excel FNGROUPCOUNT Record Remote Code Execution Vulnerability
18910	Microsoft Excel LABEL Record Remote Code Execution Vulnerability
18886	Microsoft Excel OBJECT Record Remote Code Execution Vulnerability
18853	Microsoft Excel Selection Record Remote Code Execution Vulnerability
18885	Microsoft Excel Selection Record Variant Remote Code Execution Vulnerability
18422	Microsoft Excel Unspecified Remote Code Execution Vulnerability
18500	Microsoft HLINK.DLL Link Memory Corruption Vulnerability
18858	Microsoft IIS ASP Remote Code Execution Vulnerability
18736	Microsoft Internet Explorer 7 Denial of Service Vulnerability
18773	Microsoft Internet Explorer ADODB.Recordset Filter Property Denial of Service Vulnerability
18769	Microsoft Internet Explorer HHCtrl ActiveX Control Memory Corruption Vulnerability
18820	Microsoft Internet Explorer Href Title Denial Of Service Vulnerability
18682	Microsoft Internet Explorer OuterHTML Redirection Handling Information Disclosure Vulnerability
18771	Microsoft Internet Explorer OutlookExpress.AddressBook Denial of Service Vulnerability
18583	Microsoft Office Embedded Shockwave Flash Object Security Bypass Weakness
18915	Microsoft Office Malformed GIF File Remote Code Execution Vulnerability
18913	Microsoft Office Malformed PNG File Remote Code Execution Vulnerability
18889	Microsoft Office Malformed String Parsing Code Execution Vulnerability
18911	Microsoft Office Property Code Execution Vulnerability
18912	Microsoft Office String Parsing Remote Code Execution Vulnerability
18923	Microsoft Windows DHCP Client Service Remote Code Execution Vulnerability

Bugtraq ID	Title
18424	Microsoft Windows Routing and Remote Access Unspecified Remote Code Execution Vulnerability
18863	Microsoft Windows Server Driver Mailslot Remote Heap Buffer Overflow Vulnerability
18891	Microsoft Windows Server Driver Remote Information Disclosure Vulnerability
18604	Mozilla Network Security Services Library Remote Denial of Service Vulnerability
18758	Opera Document Stylesheet Denial Of Service Vulnerability
18585	Opera Malicious HTML Processing Denial of Service Vulnerability
18692	Opera SSL Certificate Spoofing Weakness
18594	Opera Web Browser JPEG Image Handling Remote Buffer Overflow Vulnerability
18622	Yahoo! Messenger Message Handling Denial of Service Vulnerability

June 21, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 25 additional vulnerabilities. The following table includes information about the 25 additional vulnerabilities.

Bugtraq ID	Title
18098	HP-UX Software Distributor Unspecified Local Privilege Escalation Vulnerability
18303	Microsoft DXImageTransform.Microsoft.Light ActiveX Control Remote Code Execution Vulnerability
18381	Microsoft Exchange Server Outlook Web Access Script Injection Vulnerability
18328	Microsoft Internet Explorer COM Object Instantiation Code Execution Vulnerability Variant
18277	Microsoft Internet Explorer Frameset Denial of Service Vulnerability

Bugtraq ID	Title
18309	Microsoft Internet Explorer HTML Decoding Remote Code Execution Vulnerability
18112	Microsoft Internet Explorer Malformed HTML Parsing Denial of Service Vulnerability
18198	Microsoft Internet Explorer MHTML URI Buffer Overflow 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
18359	Microsoft JScript Memory Corruption Vulnerability
18382	Microsoft PowerPoint Malformed Record Remote Code Execution Vulnerability
18357	Microsoft SMB Driver Local Denial Of Service Vulnerability
18394	Microsoft Windows Malformed ART Image Remote Code Execution Vulnerability
18385	Microsoft Windows Media Player Malformed PNG 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
18389	Microsoft Windows RPC Mutual Authentication Service Spoofing Vulnerability
18356	Microsoft Windows SMB Driver Local Privilege Escalation Vulnerability
18374	Microsoft Windows TCP/IP Protocol Driver Remote Buffer Overflow Vulnerability
18228	Mozilla Firefox SeaMonkey and Thunderbird Multiple Remote Vulnerabilities
18165	Multiple Browser Marquee Denial of Service Vulnerability
18083	Multiple Browsers Exception Handling Information Disclosure Vulnerability
16770	Multiple Mozilla Products IFRAME JavaScript Execution Vulnerability
18308	Multiple Vendor Web Browser JavaScript Key Filtering Vulnerability

May 30, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 10 additional vulnerabilities. The following table includes information about the 10 additional vulnerabilities.

Bugtraq ID	Title
18057	HP-UX Kernel Unspecified Local Denial of Service Vulnerability
17926	Microsoft Infotech Storage Library Heap Corruption Vulnerability
17717	Microsoft Internet Explorer MHTML URI Handler Information Disclosure Vulnerability
17713	Microsoft Internet Explorer Modal Dialog Manipulation Vulnerability
17932	Microsoft Internet Explorer Position CSS Denial of Service Vulnerability
17820	Microsoft Internet Explorer Unspecified OBJECT Tag Memory Corruption Variant Vulnerability
18008	Microsoft Windows Impersonation Privilege Escalation Weakness
17934	Microsoft Windows Path Conversion Weakness
18037	Microsoft Word Unspecified Remote Code Execution Vulnerability
17902	Sun Solaris LibIKE IKE Exchange Denial Of Service Vulnerability

May 10, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 16 additional vulnerabilities. The following table includes information about the 16 additional vulnerabilities.

Bugtraq ID	Title
17280	HP-UX Passwd Unspecified Local Denial of Service Vulnerability
17400	HP-UX SU Local Unauthorized Access Vulnerability
17576	IBM AIX RM_MLCache_File Insecure Temporary File Creation Vulnerability
15334	Macromedia Flash ActionDefineFunction Memory Access Vulnerability
15332	Macromedia Flash Array Index Memory Access Vulnerability

Bugtraq ID	Title
17908	Microsoft Exchange Server Calendar Remote Code Execution Vulnerability
17658	Microsoft Internet Explorer Nested OBJECT Tag Memory Corruption Vulnerability
17905	Microsoft Windows MSDTC Denial Of Service Vulnerability
17906	Microsoft Windows MSDTC Invalid Memory Access Denial Of Service Vulnerability
17499	Mozilla Firefox HTML Parsing Null Pointer Dereference Denial of Service Vulnerability
17671	Mozilla Firefox iframe.contentWindow.focus Buffer Overflow Vulnerability
17516	Mozilla Suite
17513	Opera Web Browser Stylesheet Attribute Buffer Overflow Vulnerability
17479	Sun Solaris LDAP2 RootDN Password Disclosure Vulnerability
17478	Sun Solaris SH(1) Local Denial of Service Vulnerability
17313	Sun Cluster SunPlex Manager Unauthorized File Access Vulnerability

April 19, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 15 additional vulnerabilities and 3 updated vulnerabilities. The following table includes information about the 15 additional vulnerabilities.

Bugtraq ID	Title
17452	Microsoft FrontPage Server Extensions Cross-Site Scripting Vulnerability
17404	Microsoft Internet Explorer Address Bar Spoofing 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
17468	Microsoft Internet Explorer HTML Tag Memory Corruption Vulnerability

Bugtraq ID	Title
17450	Microsoft Internet Explorer Invalid HTML Parsing Code Execution Vulnerability
17457	Microsoft Internet Explorer Popup Cross-Domain Information Disclosure Vulnerability
17460	Microsoft Internet Explorer Persistent Window Content Address Bar Spoofing Vulnerability
17131	Microsoft Internet Explorer Script Action Handler Buffer Overflow Vulnerability
12960	Microsoft Jet Database Engine Malformed Database File Buffer Overflow Vulnerability
17462	Microsoft MDAC RDS.Dataspace ActiveX Control Remote Code Execution Vulnerability
17459	Microsoft Outlook Express Windows Address Book File Parsing Buffer Overflow Vulnerability
17325	Microsoft Windows Help Image Processing Heap Overflow Vulnerability
17464	Microsoft Windows Shell COM Object Remote Code Execution Vulnerability

The following table includes information about the 3 updated vulnerabilities.

Bugtraq ID	Title
17196	Microsoft Internet Explorer CreateTextRange Remote Code Execution Vulnerability
17181	Microsoft Internet Explorer Unspecified Remote HTA Execution Vulnerability
10363	Microsoft Windows XP Self-Executing Folder Vulnerability

March 28, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 6 additional vulnerabilities. The following table includes information about the 6 additional vulnerabilities.

Bugtraq ID	Title
17143	HP-UX Usermod Local Unauthorized Access Vulnerability

Bugtraq ID	Title
17115	IBM AIX MKLVCopy Unspecified Security Vulnerability
17188	Microsoft ASP.NET COM Components W3WP Remote Denial Of Service Vulnerability
17196	Microsoft Internet Explorer CreateTextRange Remote Code Execution Vulnerability
17181	Microsoft Internet Explorer Unspecified Remote HTA Execution Vulnerability
17202	RealNetworks Multiple Products Multiple Buffer Overflow Vulnerabilities

March 16, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 9 additional vulnerabilities and 5 updated vulnerabilities. The following table includes information about the 9 additional vulnerabilities.

Bugtraq ID	Title
17106	Macromedia Flash Multiple Unspecified Security Vulnerabilities
17100	Microsoft Excel Malformed Description Remote Code Execution Vulnerability
17108	Microsoft Excel Malformed Formula Size Remote Code Execution Vulnerability
17091	Microsoft Excel Malformed Parsing Format File Remote Code Execution Vulnerability
17101	Microsoft Excel Malformed Record Remote Code Execution Vulnerability
16870	Microsoft Internet Explorer IsComponentInstalled Buffer Overflow Vulnerability
16978	Microsoft Internet Explorer Java Applet Handling Denial of Service Vulnerability
17000	Microsoft Office Routing Slip Processing Remote Buffer Overflow Vulnerability
16966	Sun Solaris Proc Filesystem Pagedata Subsystem Local Denial Of Service Vulnerability

The following table includes information about the 5 updated vulnerabilities.

Bugtraq ID	Title
15780	Microsoft Excel Malformed Range Memory Corruption Vulnerability
17091	Microsoft Excel Malformed Parsing Format File Remote Code Execution Vulnerability
16181	Microsoft Excel Malformed Graphic File Code Execution Vulnerability
15926	Microsoft Excel Unspecified Memory Corruption Vulnerabilities
16484	Microsoft Windows Multiple Local Privilege Escalation Vulnerabilities

February 28, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 4 additional vulnerabilities. The following table includes information about the 4 new vulnerabilities.

Bugtraq ID	Title
16687	Microsoft Internet Explorer Script Engine Buffer Overflow Vulnerability
16782	Microsoft Word Malformed Document Denial Of Service Vulnerability
16741	Mozilla Firefox HTML Parsing Denial of Service Vulnerability
16826	Sun Solaris HSFS Filesystem Local Denial Of Service Vulnerability

February 15, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 11 additional vulnerabilities. The following table includes information about the 11 new vulnerabilities.

Bugtraq ID	Title
16584	IBM AIX ARP Local Buffer Overflow Vulnerability
16624	IBM AIX Local Kernel Denial Of Service Vulnerability
16352	Microsoft Internet Explorer Drag And Drop File Installation Vulnerability Variant
16516	Microsoft Internet Explorer WMF File Unspecified Memory Corruption Vulnerability

Bugtraq ID	Title
16634	Microsoft PowerPoint 2000 Remote Information Disclosure Vulnerability
16645	Microsoft Windows IGMPv3 Denial of Service Vulnerability
16633	Microsoft Windows Media Player Bitmap Handling Buffer Overflow Vulnerability
16644	Microsoft Windows Media Player Plugin Buffer Overflow Vulnerability
16484	Microsoft Windows Multiple Local Privilege Escalation Vulnerabilities
16636	Microsoft Windows Web Client Buffer Overflow Vulnerability
16476	Multiple Mozilla Products Memory Corruption/Code Injection/Access Restriction Bypass Vulnerabilities

February 8, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 8 additional vulnerabilities. The following table includes information about the 8 new vulnerabilities.

Bugtraq ID	Title
17701	Microsoft Excel Unspecified Code Execution Vulnerability
16409	Microsoft Internet Explorer ActiveX Control Kill Bit Bypass Vulnerability
10391	Microsoft Internet Explorer CLSID File Execution Vulnerability
16441	Microsoft Internet Explorer Flash ActionScript JScript Handling Denial of Service Vulnerability
16463	Microsoft Internet Explorer URLMon.DLL Denial Of Service Vulnerability
10691	Microsoft Internet Explorer Window.createPopup File Download Misrepresentation Vulnerability
16427	Mozilla Firefox XBL -MOZ-BINDING Property Cross-Domain Scripting Vulnerability
17696	Sun Solaris UUSTAT Local Buffer Overflow Vulnerability

January 25, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 5 additional vulnerabilities. The following table includes information about the 5 new vulnerabilities.

Bugtraq ID	Title
16316	HP-UX FTPD Remote Denial Of Service Vulnerability
16181	Microsoft Excel Unspecified Code Execution Vulnerability
16240	Microsoft Internet Explorer Malformed IMG and XML Parsing Denial of Service Vulnerability
16245	Sun Solaris LPSCHED Multiple Local Vulnerabilities
16193	Sun Solaris UUSTAT Local Buffer Overflow Vulnerability

January 11, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 6 additional vulnerabilities. The following table includes information about the 6 new vulnerabilities.

Bugtraq ID	Title
14660	Apache CGI Byterange Request Denial of Service Vulnerability
16152	Apache Mod_SSL Custom Error Document Remote Denial Of Service Vulnerability
15979	HP-UX Software Distributor Unspecified Remote Unauthorized Access Vulnerability
16197	Microsoft Outlook / Microsoft Exchange TNEF Decoding Remote Code Execution Vulnerability
16194	Microsoft Windows Embedded Web Font Buffer Overflow Vulnerability
16167	Microsoft Windows Graphics Rendering Engine Multiple Memory Corruption Vulnerabilities

January 4, 2006

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 5 additional vulnerabilities. The following table includes information about the 5 new vulnerabilities.

Bugtraq ID	Title
16070	Microsoft Internet Explorer HTML Parsing Denial of Service Vulnerabilities
16079	Microsoft Internet Explorer MSHTML.DLL HTML Parsing Denial of Service Vulnerability
16074	Microsoft Windows Graphics Rendering Engine WMF SetAbortProc Code Execution Vulnerability
16102	IBM AIX GetShell and GetCommand File Enumeration Vulnerability
16103	IBM AIX GetShell and GetCommand Partial File Disclosure Vulnerability

December 20, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 16 additional vulnerabilities. The following table includes information about the 16 new vulnerabilities.

Bugtraq ID	Title
15834	Apache Mod_IMAP Referer Cross-Site Scripting Vulnerability
15762	Apache MPM Worker.C Denial Of Service Vulnerability
15759	HP-UX Unspecified IPSec Unauthorized Remote Access Vulnerability
15930	HP-UX WBEM Services Denial of Service Vulnerability
15926	Microsoft Excel Unspecified Memory Corruption Vulnerabilities
15780	Microsoft Excel Unspecified Memory Corruption Vulnerability
15921	Microsoft Internet Information Server 5.1 DLL Request Denial of Service Vulnerability
15773	Mozilla Firefox Large History File Buffer Overflow Vulnerability
15835	Opera Web Browser Download Dialog Manipulation File Execution Vulnerability
15813	Opera Web Browser Long Title Element Bookmark Denial of Service Vulnerability

Bugtraq ID	Title
15881	IBM AIX Debug Malloc Tools Local Buffer Overflow Vulnerability
15880	IBM AIX GetShell and GetCommand Arbitrary File Overwrite Vulnerability
15879	IBM AIX MUXATMD Local Buffer Overflow Vulnerability
15878	IBM AIX slocal Local Buffer Overflow Vulnerability
15758	IBM AIX UMOUNTALL Unspecified Absolute Path Security Vulnerability
15691	Real Networks RealPlayer Unspecified Remote Code Execution Vulnerability

December 13, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 4 additional vulnerabilities and 1 updated vulnerability. The following table includes information about the 4 new vulnerabilities.

Bugtraq ID	Title
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
15826	Microsoft Windows Asynchronous Procedure Call Local Privilege Escalation Vulnerability

Updated vulnerability

The following table includes information about the 1 updated vulnerability.

Bugtraq ID	Title
13799	Microsoft Internet Explorer JavaScript OnLoad Handler Remote Code Execution Vulnerability

December 7, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 8 additional vulnerabilities. The following table includes information about the 8 new vulnerabilities.

Bugtraq ID	Title
15474	HP-UX IKE Exchange Denial Of Service Vulnerabilities
15397	IBM AIX Diagela.SH Unspecified Security Vulnerability
15660	Microsoft Internet Explorer CSS Import Cross-Domain Restriction Bypass Vulnerability
15671	Microsoft Windows CreateRemoteThread Local Denial of Service Vulnerability
15613	Microsoft Windows SynAttackProtect Predictable Hash Remote Denial of Service Vulnerability
15448	Multiple Vendor IpCommandLine Application Path Vulnerability
15521	Opera Web Browser Arbitrary Command Execution Vulnerability
15472	Opera Web Browser HTML Form Status Bar Misrepresentation Vulnerability

November 22, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 11 additional vulnerabilities. The following table includes information about the 11 new vulnerabilities.

Bugtraq ID	Title
15323	IBM AIX SWCONS Local Buffer Overflow Vulnerability
15331	Multiple Vendor Web Browser Cookie Hostname Handling Weakness
15359	HP-UX ENV D Local Privilege Escalation Vulnerability
15366	HP-UX RemSHD Unspecified Unauthorized Access Vulnerability
15381	RealNetworks RealOne Player/RealPlayer RM File Remote Stack Based Buffer Overflow Vulnerability
15382	RealNetworks RealPlayer DUNZIP32.DLL Heap Overflow Vulnerability
15384	Sun Solaris In. Named Remote Denial of Service Vulnerability

Bugtraq ID	Title
15398	RealNetworks RealPlayer Unspecified Malformed Image Skin File Buffer Overflow
15412	HP-UX XTerm Unspecified Local Unauthorized Access Vulnerability
15420	Sun Solaris LibIKE IKE Exchange Denial of Service Vulnerability
15460	Microsoft Windows Plug and Play Denial of Service Vulnerability

November 8, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 8 additional vulnerabilities and 1 updated vulnerability. The following table includes information about the 8 new vulnerabilities.

Bugtraq ID	Title
15247	IBM AIX CHCONS Local Buffer Overflow Vulnerability
15138	HP-UX FTP Server Directory Listing Vulnerability
15136	HP-UX LPD Arbitrary Command Execution Vulnerability
15208	Microsoft Internet Explorer Java Applet Denial of Service Vulnerability
15268	Microsoft Internet Explorer Malformed HTML Parsing Denial of Service Vulnerability
15356	Microsoft Windows Graphics Rendering Engine WMF Format Code Execution Vulnerability
15352	Microsoft Windows Graphics Rendering Engine WMF/EMF Format Code Execution Vulnerability
15222	Sun Solaris Management Console HTTP TRACE Information Disclosure Vulnerability

Updated vulnerability

The following table includes information about the 1 updated vulnerability.

Bugtraq ID	Title
12834	Microsoft Windows Graphical Device Interface Library Denial Of Service Vulnerability

October 25, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 6 additional vulnerabilities. The following table includes information about the 6 new vulnerabilities.

Bugtraq ID	Title
15105	IBM AIX LSCFG Insecure Temporary File Creation Vulnerability
15130	Microsoft Windows Unspecified Remote Code Execution Vulnerability
15008	Microsoft Windows Wireless Zero Configuration Service Information Disclosure Vulnerability
15015	Mozilla Firefox IFRAME Handling Denial Of Service Vulnerability
15029	Mozilla Firefox Multiple Unspecified Vulnerabilities
15124	Opera Web Browser Multiple Malformed HTML Parsing Denial Of Service Vulnerabilities

October 11, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 16 additional vulnerabilities and 3 updated vulnerabilities. The following table includes information about the 16 new vulnerabilities.

Bugtraq ID	Title
14959	IBM AIX Getconf Local Buffer Overflow Vulnerability
15067	Microsoft Collaboration Data Objects Remote Buffer Overflow Vulnerability
15063	Microsoft DirectX DirectShow AVI Processing Buffer Overflow Vulnerability
15061	Microsoft Internet Explorer COM Object Instantiation Variant Vulnerability
14969	Microsoft Internet Explorer XmlHttpRequest Parameter Validation Weakness
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	Title
15066	Microsoft Windows Client Service For Netware Buffer Overflow Vulnerability
15064	Microsoft Windows Explorer Web View Script Injection Vulnerability
15069	Microsoft Windows Malicious Shortcut Handling Remote Code Execution Vulnerability
15070	Microsoft Windows Malicious Shortcut Handling Remote Code Execution Variant Vulnerability
15056	Microsoft Windows MSDTC Memory Corruption Vulnerability
15065	Microsoft Windows Plug And Play UMPNPMGR.DLL wsprintFW Buffer Overflow Vulnerability
14963	OpenSSH LoginGraceTime Remote Denial Of Service Vulnerability
14949	Sun Solaris Xsun and Xprt Local Privilege Escalation Vulnerability

Updated vulnerabilities

The following table includes information about the 3 updated vulnerabilities.

Bugtraq ID	Title
14594	Microsoft Visual Studio .NET msdds.dll Remote Code Execution Vulnerability
14260	Microsoft Windows Network Connections Manager Library Local Denial of Service Vulnerability
12160	Microsoft Windows FTP Client Directory Traversal Vulnerability

September 27, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 14 additional vulnerabilities and 4 updated vulnerabilities. The following table includes information about the 14 new vulnerabilities.

Bugtraq ID	Title
14856	Microsoft Internet Explorer Unspecified Code Execution Vulnerability
14888	Mozilla Browser/Firefox Arbitrary Command Execution Vulnerability
14923	Mozilla Browser/Firefox Arbitrary HTTP Request Injection Vulnerability

Bugtraq ID	Title
14920	Mozilla Browser/Firefox Chrome Page Loading Restriction Bypass Privilege Escalation Weakness
14919	Mozilla Browser/Firefox Chrome Window Spoofing Vulnerability
14921	Mozilla Browser/Firefox DOM Objects Spoofing Vulnerability
14917	Mozilla Browser/Firefox Unspecified JavaScript Engine Integer Overflow Vulnerability
14916	Mozilla Browser/Firefox XBM Image Processing Heap Overflow Vulnerability
14918	Mozilla Browser/Firefox Zero-Width Non-Joiner Stack Corruption Vulnerability
14924	Multiple Browser Proxy Auto-Config Script Handling Remote Denial of Service Vulnerability
14880	Opera Web Browser Mail Client Multiple Vulnerabilities
14884	Opera Web Browser Unspecified Drag And Drop File Upload Vulnerability
14620	PCRE Regular Expression Heap Overflow Vulnerability
14915	Sun Solaris UFS Local Denial of Service Vulnerability

Updated vulnerabilities

The following table includes information about the 4 updated vulnerabilities.

Bugtraq ID	Title
13022	IBM AIX NIS Client Unspecified Remote Vulnerability
12075	libTIFF Heap Corruption Integer Overflow Vulnerabilities
11406	LibTIFF Multiple Buffer Overflow Vulnerabilities
14239	MIT Kerberos 5 KRB5_Recvauth Remote Pre-Authentication Double-Free Vulnerability

September 14, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 8 additional vulnerabilities. The following table includes information about the 8 new vulnerabilities.

Bugtraq ID	Title
14721	Apache Mod_SSL SSLVerifyClient Restriction Bypass Vulnerability
14772	Microsoft Exchange Server 2003 Exchange Information Store Denial Of Service Vulnerability
14764	Microsoft IIS WebDAV HTTP Request Source Code Disclosure Vulnerability
14755	Microsoft Internet Explorer Unspecified Remote Code Execution Vulnerability
14683	Microsoft Internet Explorer Unspecified Remote Vulnerability
14743	Microsoft Windows Keyboard Event Privilege Escalation Weakness
14784	Mozilla/Netscape/Firefox Browsers Domain Name Remote Buffer Overflow Vulnerability
14729	OpenSSH GSSAPI Credential Disclosure Vulnerability

August 30, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 1 additional vulnerability. The following table includes information about the 1 new vulnerability.

Bugtraq ID	Title
14594	Microsoft Visual Studio .NET msdds.dll Remote Code Execution Vulnerability

August 23, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 6 additional vulnerabilities. The following table includes information about the 6 new vulnerabilities.

Bugtraq ID	Title
14480	Microsoft Windows Unspecified Remote Arbitrary Code Execution Vulnerability
14526	Mozilla Firefox And Thunderbird Long URI Obfuscation Weakness
14443	Mozilla Suite Firefox and Thunderbird Debug Mode Insecure Temporary File Creation Vulnerability
14410	Opera Web Browser Image Dragging Cross-Domain Scripting and File Retrieval Vulnerability
14402	Opera Web Browser Content-Disposition Header Download Dialog File Extension Spoofing Vulnerability
14510	Sun Solaris Printed Arbitrary File Deletion Vulnerability

August 11, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 17 additional vulnerabilities and 1 updated vulnerability. The following table includes information about the 17 new vulnerabilities.

Bugtraq ID	Title
12996	GNU GZip CHMod File Permission Modification Race Condition Weakness
13290	GNU GZip Filename Directory Traversal Vulnerability
14511	Microsoft Internet Explorer COM Object Instantiation 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
14282	Microsoft Internet Explorer JPEG Image Rendering Unspecified Buffer Overflow Vulnerability

Bugtraq ID	Title
14286	Microsoft Internet Explorer JPEG Image Rendering Unspecified Denial Of Service Vulnerability
14515	Microsoft Internet Explorer Unspecified SharePoint Portal Services Log Sink ActiveX Vulnerability
14512	Microsoft Internet Explorer Web Folder Behaviors Cross-Domain Scripting Vulnerability
14288	Microsoft MSN Messenger / Internet Explorer Image ICC Profile Processing Vulnerability
14519	Microsoft Windows Kerberos Denial Of Service Vulnerability
14520	Microsoft Windows Kerberos PKINIT Man In The Middle Vulnerability
14518	Microsoft Windows Telephony Service Buffer Overflow Vulnerability
14513	Microsoft Windows Plug and Play Buffer Overflow Vulnerability
14514	Microsoft Windows Print Spooler Buffer Overflow Vulnerability
14376	Microsoft Windows Unspecified USB Driver Buffer Overflow Vulnerability
14325	Mozilla Firefox Weak Authentication Mechanism Vulnerability

Updated vulnerability

The following table includes information about the 1 updated vulnerability.

Bugtraq ID	Title
14259	Microsoft Windows Kernel Unspecified Remote Desktop Protocol Denial Of Service Vulnerability

July 21, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 10 additional vulnerabilities. The following table includes information about the 10 new vulnerabilities.

Bugtraq ID	Title
14217	Microsoft ASP.NET RPC/Encoded Remote Denial Of Service Vulnerability
14225	Microsoft Outlook Express Multiple Vulnerabilities

Bugtraq ID	Title
14259	Microsoft Windows Kernel Unspecified Remote Denial Of Service Vulnerability
14178	Microsoft Windows MSRPC Eventlog Information Disclosure Vulnerability
14177	Microsoft Windows MSRPC SVCCTL Service Enumeration Vulnerability
14260	Microsoft Windows Network Connections Manager Library Local Denial of Service Vulnerability
14240	MIT Kerberos 5 Key Distribution Center Remote Denial of Service Vulnerability
14236	MIT Kerberos 5 Key Distribution Center Remote Single Byte Heap Overflow Vulnerability
14239	MIT Kerberos 5 KRB5_Recvauth Remote Pre-Authentication Double-Free Vulnerability
14242	Mozilla Suite Firefox And Thunderbird Multiple Vulnerabilities

July 13, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 11 additional vulnerabilities. The following table includes information about the 11 new vulnerabilities.

Bugtraq ID	Title
14106	Apache HTTP Request Smuggling Vulnerability
13774	HP-UX Trusted System Unspecified Remote Unauthorized Access Vulnerability
14007	Microsoft Internet Explorer Dialog Box Origin Spoofing Vulnerability
14087	Microsoft Internet Explorer Javaprx.dll COM Object Instantiation Heap Overflow Vulnerability
12646	Microsoft Log Sink Class ActiveX Control Arbitrary File Creation Vulnerability
14093	Microsoft Update Rollup 1 for Windows 2000 SP4 Released - Multiple Vulnerabilities Fixed
14214	Microsoft Windows Color Management Module ICC Profile Buffer Overflow Vulnerability

Bugtraq ID	Title
14216	Microsoft Word Malformed Document Font Processing Buffer Overflow Vulnerability
14008	Mozilla/Firefox Browsers Dialog Box Origin Spoofing Vulnerability
14073	RealNetworks Real and RealOne Player Unspecified MP3 ActiveX Control Execution Vulnerability
14048	RealNetworks RealPlayer RealText Parsing Heap Overflow Vulnerability

June 28, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 22 additional vulnerabilities and 2 updated vulnerabilities. The following table includes information about the 22 new vulnerabilities.

Bugtraq ID	Title
13778	Apache HTTPd Password Command Line Argument Buffer Overflow Vulnerability
13777	Apache HTTPd User Command Line Argument Buffer Overflow Vulnerability
13912	IBM AIX diagTasksWebSM Command Line Argument Local Buffer Overflow Vulnerability
13914	IBM AIX GetLVName Command Line Argument Local Buffer Overflow Vulnerability
13909	IBM AIX Invsout Local Buffer Overflow Vulnerability
13911	IBM AIX PAGINIT Local Format String Vulnerability
13919	IBM AIX Pdelay Command Line Argument Local Buffer Overflow Vulnerability
13916	IBM AIX Pdisable Command Line Argument Local Buffer Overflow Vulnerability
13915	IBM AIX Penable Command Line Argument Local Buffer Overflow Vulnerability
13918	IBM AIX Phold Command Line Argument Local Buffer Overflow Vulnerability
13920	IBM AIX Pshare Command Line Argument Local Buffer Overflow Vulnerability

Bugtraq ID	Title
13917	IBM AIX Pstart Command Line Argument Local Buffer Overflow Vulnerability
13921	IBM AIX Swcons Command Line Argument Local Buffer Overflow Vulnerability
13799	Microsoft Internet Explorer JavaScript OnLoad Handler Denial of Service Vulnerability
13800	Microsoft Internet Explorer Object Embedding Denial of Service Vulnerability
13798	Microsoft Internet Explorer Restricted Sites Malformed URI Denial of Service Vulnerability
13846	Microsoft ISA Server SecureNAT Unspecified Denial Of Service Vulnerability
13837	Microsoft Outlook Express Attachment Processing File Extension Obfuscation Vulnerability
13801	Microsoft Windows XP Windows Management Instrumentation Denial of Service Vulnerability
13873	Multiple Vendor Multiple HTTP Request Smuggling Vulnerabilities
13758	Sun CDE DtSvc DTDataBaseSearchPath Unspecified Buffer Overflow Vulnerability
13757	Sun CDE DtSvc Unspecified Buffer Overflow Vulnerability

Updated vulnerabilities

The following table includes information about the 2 updated vulnerabilities.

Bugtraq ID	Title
8231	CGI.pm Start_Form Cross-Site Scripting Vulnerability
6111	Safe.PM Unsafe Code Execution Vulnerability

June 15, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 19 additional vulnerabilities and 1 updated vulnerability. The following table includes information about the 19 new vulnerabilities.

Bugtraq ID	Title
13952	Microsoft Exchange Server Outlook Web Access HTML Injection Vulnerability
13948	Microsoft Agent Trusted Content Spoofing Vulnerability
13955	Microsoft ISA Server HTTP/HTTPS Service Basic Auth Information Disclosure Vulnerability
13950	Microsoft Windows Web Client Service Remote Code Execution Vulnerability
13953	Microsoft Windows HTML Help Remote Code Execution Vulnerability
13947	Microsoft Internet Explorer Unspecified GIF And BMP Denial Of Service Vulnerability
13946	Microsoft Internet Explorer Unspecified DigWebX ActiveX Control Vulnerability
13943	Microsoft Internet Explorer XML Redirect Information Disclosure Vulnerability
13956	Microsoft ISA Server HTTP Request Smuggling Vulnerability
13954	Microsoft ISA Server NetBIOS Predefined Filter Policy Bypass Vulnerability
13940	Multiple Vendor Telnet Client Remote Information Disclosure Vulnerability
13941	Microsoft Internet Explorer PNG Image Rendering Buffer Overflow Vulnerability
13951	Microsoft Outlook Express NNTP Response Parsing Buffer Overflow Vulnerability
13942	Microsoft Incoming SMB Packet Validation Remote Buffer Overflow Vulnerability
13755	Sun Solaris BCP LibMLE Unspecified Buffer Overflow Vulnerability
13732	Sun Solaris ATOK12 Unspecified Insecure File/Directory Permissions Vulnerability

Bugtraq ID	Title
13731	Sun Solaris JServer Unspecified Buffer Overflow Vulnerability
13748	Sun Solaris XML Library Unspecified Buffer Overflow Vulnerability
13735	Sun Solaris ATOK12 Unspecified Buffer Overflow Vulnerability

Updated vulnerabilities

The following table includes information about the 1 updated vulnerability.

Bugtraq ID	Title
13122	Microsoft Word Malformed Document Buffer Overflow Vulnerability

June 7, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 21 additional vulnerabilities. The following table includes information about the 21 new vulnerabilities.

Bugtraq ID	Title
13677	Microsoft Outlook HTML Email URI Spoofing Vulnerability
13687	Microsoft Word MCW File Handler Buffer Overflow Vulnerability
2866	Multiple Vendor Libcurses Buffer Overflow Vulnerability
2581	Solaris IPCS Timezone Buffer Overflow Vulnerability
13724	Sun Basic Security Module Audit_warn Warning Message Email Failure Weakness
13747	Sun Solaris BSMUNCONV Root Crontab Overwrite Vulnerability
13743	Sun Solaris Directory Creation Kernel Panic Vulnerability
13721	Sun Solaris IN.RSHD Unauthorized Connection Vulnerability
13740	Sun Solaris LLC2 Network Driver Multicast Packet Denial Of Service Vulnerability
13752	Sun Solaris Local Fopen() Denial Of Service Vulnerability
13744	Sun Solaris Mailx Unspecified Vulnerability
13746	Sun Solaris Missing KRB5.CONF Unauthorized Login Vulnerability

Bugtraq ID	Title
13745	Sun Solaris Powerd Unspecified Buffer Overflow Vulnerability
13751	Sun Solaris Remote Unspecified DCS Denial Of Service Vulnerability
13719	Sun Solaris RMFormat Unspecified Buffer Overflow Vulnerabilities
13718	Sun Solaris SDTSmartCardAdmin Unspecified Security Vulnerability
13750	Sun Solaris SSH IKE Information Disclosure Vulnerability
13741	Sun Solaris Smart Card PAM.CONF Lowered Security Settings Vulnerability
13726	Sun Solaris Unspecified OCFServ Vulnerability
13738	Sun Solaris USB Attachment Points Insecure Default Permissions Vulnerability
13734	Sun TTYMux Kernel Memory Disclosure Vulnerability

May 24, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 12 additional vulnerabilities. The following table includes information about the 12 new vulnerabilities.

Bugtraq ID	Title
13537	Apache HTTDigest Realm Command Line Argument Buffer Overflow Vulnerability
13658	Microsoft IPV6 TCPIP Loopback LAND Denial of Service Vulnerability
13564	Microsoft SQL Server 2000 Multiple Vulnerabilities
13607	Microsoft Windows Media Player Digital Rights Management Arbitrary Web Page Launch Weakness
13544	Mozilla Firefox Install Method Remote Arbitrary Code Execution Vulnerability
13645	Mozilla Suite And Firefox DOM Property Overrides Code Execution Vulnerability
13641	Mozilla Suite And Firefox Multiple Script Manager Security Bypass Vulnerabilities
13676	Multiple Vendor TCP Timestamp PAWS Remote Denial Of Service Vulnerability

Bugtraq ID	Title
13530	RealNetworks RealPlayer Unspecified Code Execution Vulnerability
13588	Sun Solaris automountd Local Denial Of Service Vulnerability
13552	Sun Solaris NIS+ Unspecified Remote Denial Of Service Vulnerability
13626	Yahoo! Messenger URL Handler Remote Denial Of Service Vulnerability

May 11, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 10 additional vulnerabilities and 4 updated vulnerabilities. The following table includes information about the 10 new vulnerabilities.

Bugtraq ID	Title
12651	HP-UX FTP Server Unspecified Restricted File Access Vulnerability
13367	HP-UX ICMP PMTUD Remote Denial Of Service Vulnerability
10630	HP-UX ObAM WebAdmin Unspecified Unauthorized Access Vulnerability
10791	HP-UX SMTKFONT Remote Unauthorized Access Vulnerability
11493	HP-UX STMKFONT Local Privilege Escalation Vulnerability
10631	HP-UX Undisclosed ARPA Transport Local Denial Of Service Vulnerability
10790	HP-UX XFS Remote Unauthorized Access Vulnerability
12075	libTIFF Heap Corruption Integer Overflow Vulnerabilities
11406	LibTIFF Multiple Buffer Overflow Vulnerabilities
13300	Microsoft Windows ASN.1 Library Bit String Processing Variant Heap Corruption Vulnerability

Updated vulnerabilities

The following table includes information about 4 updated vulnerabilities.

Bugtraq ID	Title
9109	Microsoft Internet Explorer BackToFramedJPU Cross-Domain Policy Vulnerability

Bugtraq ID	Title
9568	Microsoft Internet Explorer NavigateAndFind() Cross-Zone Policy Vulnerability
13248	Microsoft Windows Explorer Preview Pane Script Injection Vulnerability
9182	Multiple Browser URI Display Obfuscation Weakness

April 26, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 19 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
13204	IBM AIX Journaled File System Memory Disclosure Vulnerability
13022	IBM AIX NIS Client Unspecified Remote Vulnerability
13248	Microsoft Windows Explorer Preview Pane Script Injection Vulnerability
13228	Mozilla Firefox PLUGINSFRAME Remote Script Code Execution Vulnerability
13231	Mozilla Firefox Search Target Sidebar Panel Script Code Execution Vulnerability
13229	Mozilla Suite And Firefox Blocked Pop-Up Window Remote Script Code Execution Vulnerability
13233	Mozilla Suite And Firefox Document Object Model Nodes Code Execution Vulnerability
13216	Mozilla Suite And Firefox Favicon Link Tag Remote Script Code Execution Vulnerability
13230	Mozilla Suite And Firefox Global Scope Pollution Cross-Site Scripting Vulnerability
13211	Mozilla Suite And Firefox Search Plug-In Remote Script Code Execution Vulnerability
13232	Mozilla Suite And Firefox XPInstall JavaScript Object Instance Validation Vulnerability
10183	Multiple Vendor TCP Sequence Number Approximation Vulnerability

Bugtraq ID	Title
13215	Multiple Vendor TCP Session Acknowledgement Number Denial Of Service Vulnerability
13124	Multiple Vendor TCP/IP Implementation ICMP Remote Denial Of Service Vulnerabilities
12918	Multiple Vendor Telnet Client LINEMODE Sub-Options Remote Buffer Overflow Vulnerability
13176	Opera SSL Security Feature Design Error Vulnerability
13189	Sun Solaris libgss Unspecified Privilege Escalation Vulnerability
13241	Sun Solaris Non-Privileged Network Port Hijacking Vulnerability
13016	Sun Solaris XView Local Arbitrary File Corruption Vulnerability

April 14, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 23 additional vulnerabilities and 3 updated vulnerabilities. The following table includes information about the 23 new vulnerabilities.

Bugtraq ID	Title
12992	IBM AIX RC.BOOT Local Insecure Temporary File Creation Vulnerability
12764	Microsoft Exchange Server Mail Box Sub Folder Denial Of Service Vulnerability
13118	Microsoft Exchange Server SMTP Extended Verb Buffer Overflow Vulnerability
13117	Microsoft Internet Explorer Content Advisor File Handling Buffer Overflow Vulnerability
13120	Microsoft Internet Explorer DHTML Object Race Condition Memory Corruption Vulnerability
13123	Microsoft Internet Explorer Malformed URI Buffer Overflow Vulnerability
13114	Microsoft MSN Messenger GIF Image Processing Remote Buffer Overflow Vulnerability
13078	Microsoft Outlook and Outlook Web Access Source Email Address Spoofing Weakness

Bugtraq ID	Title
13116	Microsoft Windows Internet Protocol Validation Remote Code Execution Vulnerability
13121	Microsoft Windows Kernel Access Validation Request Buffer Overflow Vulnerability
13115	Microsoft Windows Kernel CSRSS Local Privilege Escalation Vulnerability
13109	Microsoft Windows Kernel Font Buffer Overflow Vulnerability
13110	Microsoft Windows Kernel Object Management Denial Of Service Vulnerability
10913	Microsoft Windows Large Image Processing Remote Denial Of Service Vulnerability
13112	Microsoft Windows Message Queuing Remote Buffer Overflow Vulnerability
12972	Microsoft Windows Server 2003 Service Pack 1 Released - Multiple Vulnerabilities Fixed
13008	Microsoft Windows Server 2003 SMB Redirector Local Denial Of Service Vulnerability
13132	Microsoft Windows Shell Remote Code Execution Vulnerability
12969	Microsoft Windows UNC Path Handling Unspecified Buffer Overflow Vulnerability
12889	Microsoft Windows XP TSShutdown.exe Remote Denial of Service Vulnerability
13122	Microsoft Word Malformed Document Buffer Overflow Vulnerability
13119	Microsoft Word Unspecified Document File Buffer Overflow Vulnerability
12988	Mozilla Suite/Firefox JavaScript Lambda Replace Heap Memory Disclosure Vulnerability

Updated vulnerabilities

The following table includes information about 3 updated vulnerabilities.

Bugtraq ID	Title
11264	IBM CTSTRTCASD Utility Local File Corruption Vulnerability
11196	LibXpm Image Decoding Multiple Remote Buffer Overflow Vulnerabilities

Bugtraq ID	Title
2666	Multiple Vendor loopback (land.c) Denial of Service Vulnerability

March 31, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 15 additional vulnerabilities and 9 updated vulnerabilities. The following tables include information about the vulnerabilities.

Bugtraq ID	Title
12877	Apache mod_ssl ssl_io_filter_cleanup Remote Denial Of Service Vulnerability
12834	Microsoft Windows Graphical Device Interface Library Denial Of Service Vulnerability
12870	Microsoft Windows Local Denial Of Service Vulnerability
12889	Microsoft Windows XP TSShutdown.exe Remote Denial of Service Vulnerability
12059	MIT Kerberos 5 Administration Library Add_To_History Heap-Based Buffer Overflow Vulnerability
12885	Mozilla Browser Remote Insecure XUL Start Up Script Loading Vulnerability
12672	Mozilla Firefox Address Bar Image Dragging Remote Script Execution Vulnerability
12884	Mozilla Firefox Sidebar Panel Script Injection Vulnerability
12881	Mozilla GIF Image Processing Library Remote Heap Overflow Vulnerability
12723	Multiple Browser Information Disclosure Weakness
12701	PHP Glob Function Local Information Disclosure Vulnerability
12698	RealNetworks RealOne Player/RealPlayer SMIL File Remote Stack Based Buffer Overflow Vulnerability
12697	RealNetworks RealOne Player/RealPlayer Unspecified WAV File Processing Buffer Overflow Vulnerability
12838	Sun Solaris NewGRP Local Buffer Overflow Vulnerability

Bugtraq ID	Title
12750	Yahoo! Messenger Offline Mode Status Remote Buffer Overflow Vulnerability

Updated vulnerabilities

The following table includes information about 9 updated vulnerabilities.

Bugtraq ID	Title
10857	LibPNG Graphics Library Multiple Remote Vulnerabilities
9109	Microsoft Internet Explorer BackToFramedJPU Cross-Domain Policy Vulnerability
9568	Microsoft Internet Explorer NavigateAndFind() Cross-Zone Policy Vulnerability
6961	Microsoft Internet Explorer Self Executing HTML File Vulnerability
9105	Microsoft Outlook Express MHTML Forced File Execution Vulnerability
9107	Microsoft Outlook Express MHTML Redirection Local File Parsing Vulnerability
8263	Microsoft Windows Media Player IE Zone Access Control Bypass Vulnerability
9510	Microsoft Windows Shell CLSID File Extension Misrepresentation Vulnerability
9182	Multiple Browser URI Display Obfuscation Weakness

March 23, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 4 additional vulnerabilities and 6 updated vulnerabilities. The following tables include information about the vulnerabilities.

Bugtraq ID	Title
12764	Microsoft Exchange Server Mail Box Sub Folder Denial Of Service Vulnerability

Bugtraq ID	Title
12765	Microsoft Internet Explorer MSHTML.DLL CSS Handling Remote Buffer Overflow Vulnerability
12728	Mozilla Suite/Firefox HTTP Authentication Dialogs Tab Focus Vulnerability
12798	Mozilla Suite/Firefox/Thunderbird Nested Anchor Tag Status Bar Spoofing Weakness

Updated vulnerabilities

The following table includes information about 6 updated vulnerabilities.

Bugtraq ID	Title
6961	Microsoft Internet Explorer Self Executing HTML File Vulnerability
9105	Microsoft Outlook Express MHTML Forced File Execution Vulnerability
9107	Microsoft Outlook Express MHTML Redirection Local File Parsing Vulnerability
12094	Microsoft Windows ANI File Denial of Service Vulnerability
8263	Microsoft Windows Media Player IE Zone Access Control Bypass Vulnerability
10708	Microsoft Windows Task Scheduler Remote Buffer Overflow Vulnerability

March 8, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 15 additional vulnerabilities. The following table include information about the vulnerabilities.

Bugtraq ID	Title
12574	Microsoft ASP.NET Unicode Character Conversion Multiple Cross-Site Scripting Vulnerabilities
12544	Microsoft Internet Explorer Favorites List Script Code Execution Vulnerability
12565	Microsoft Internet Explorer Malformed File URI Denial of Service Vulnerability

Bugtraq ID	Title
12541	Microsoft Internet Explorer Mouse Event URI Status Bar Obfuscation Weakness
12602	Microsoft Internet Explorer Pop-up Window Title Bar Spoofing Weakness
12641	Microsoft Windows 2000 Group Policy Bypass Vulnerability
12655	Mozilla Firefox Scrollbar Remote Code Execution Vulnerability
12659	Mozilla Suite Multiple Remote Vulnerabilities
12550	Opera Web Browser Multiple Remote Vulnerabilities
12426	Perl SuidPerl Multiple Local Vulnerabilities
12553	Sun Solaris ARP Handling Remote Denial Of Service Vulnerability
12605	Sun Solaris KCMS_Configure Unspecified Arbitrary File Corruption Vulnerability
12656	Sun Solaris STFontServerD File Corruption Vulnerability
12587	Yahoo! Messenger Download Dialogue Box File Name Spoofing Vulnerability
12585	Yahoo! Messenger Local Insecure Default Installation Vulnerability

February 22, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 17 additional vulnerabilities. The following table include information about the vulnerabilities.

Bugtraq ID	Title
12533	Firefox Remote SMB Document Local File Disclosure Vulnerability
12496	IBM AIX AuditSelect Local Format String Vulnerability
12472	IBM AIX Multiple Device Management Utilities Local Format String Vulnerability
12516	IBM AIX IPL_Varyon Local Buffer Overflow Vulnerability
12513	IBM AIX LSPath Unauthorized Local File Disclosure Vulnerability
12517	IBM AIX Netpmon Command Line Argument Local Buffer Overflow Vulnerability
12415	IBM AIX NIS Client Unspecified Remote Code Execution Vulnerability

Bugtraq ID	Title
12530	Microsoft Internet Explorer Multiple Vulnerabilities
12506	Microsoft MSN Messenger/Windows Messenger PNG Buffer Overflow Vulnerability
12459	Microsoft Outlook Web Access Login Form Remote URI Redirection Vulnerability
12466	Mozilla Firefox About Configuration Hidden Frame Remote Configuration Manipulation Vulnerability
12468	Mozilla Firefox Drag And Drop Security Policy Bypass Vulnerability
12465	Mozilla Mozilla/Firefox Cross-Domain Tab Window Script Execution Vulnerability
12470	Multiple Mozilla Browser enable.IDN Setting Weakness
12461	Multiple Web Browser International Domain Name Handling Site Property Spoofing Vulnerabilities
12315	RealNetworks RealOne Player And RealPlayer Multiple Potential Vulnerabilities
12410	RealNetworks RealPlayer Drag And Drop Zone Bypass Vulnerability

February 10, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 18 additional vulnerabilities and 5 updated vulnerabilities. The following tables include information about the vulnerabilities.

Bugtraq ID	Title
12294	Microsoft Internet Explorer Remote Information Disclosure Vulnerability
12308	Apache Utilities Insecure Temporary File Creation Vulnerability
12311	RealNetworks RealOne Player And RealPlayer ShowPreferences Action Buffer Overflow Vulnerability
12331	Netscape Navigator Infinite Array Sort Denial of Service Vulnerability
12385	Sun Solaris UDP Processing Local Denial Of Service Vulnerability
12407	Multiple Mozilla/Firefox/Thunderbird Vulnerabilities
12427	Microsoft Internet Explorer AddChannel Cross-Zone Scripting Vulnerability

Bugtraq ID	Title
12473	Microsoft Internet Explorer URI Decoding Vulnerability
12475	Microsoft Internet Explorer DHTML Method Buffer Overflow Vulnerability
12477	Microsoft Internet Explorer Unspecified ActiveX Image Control Vulnerability
12479	Microsoft Windows Hyperlink Object Library Buffer Overflow Vulnerability
12480	Microsoft Office XP HTML Link Processing Remote Buffer Overflow Vulnerability
12481	Microsoft Windows License Logging Service Buffer Overflow Vulnerability
12483	Microsoft Windows COM Structured Storage Local Privilege Escalation Vulnerability
12484	Microsoft Windows Server Message Block Handlers Remote Code Execution Vulnerability
12485	Microsoft Windows Media Player Remote PNG Image Format Buffer Overflow Vulnerability
12486	Microsoft Windows Named Pipe Remote Information Disclosure Vulnerability
12488	Microsoft OLE Remote Buffer Overflow Vulnerability

Updated vulnerabilities

Bugtraq ID	Title
10517	Multiple Browser URI Obfuscation Weakness
10973	Microsoft Internet Explorer Implicit Drag and Drop File Installation Vulnerability
11466	Microsoft Internet Explorer Valid File Drag and Drop Embedded Code Vulnerability
11950	Microsoft Windows DHTML Edit Control Script Injection Vulnerability
9108	Microsoft Internet Explorer Method Caching Mouse Click Event Hijacking Vulnerability

January 25, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 6 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
12186	Microsoft Multiple Unspecified Security Vulnerabilities
12223	Microsoft Office Encrypted Documents RC4 Initialization Vector Implementation Vulnerability
12233	Microsoft Windows User32.DLL ANI File Header Handling Stack-Based Buffer Overflow Vulnerability
12234	Mozilla/Netscape/Firefox Browser Modal Dialog Spoofing Vulnerability
12264	Microsoft Internet Explorer Dynamic IFRAME File Download Security Warning Bypass Weakness
12260	Sun Solaris Management Console User Interface Insecure Account Creation Vulnerability

January 12, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 1 additional vulnerability and 3 updated vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
12094	Microsoft Windows ANI File Denial of Service Vulnerability
11467	Microsoft Windows HTML Help Control Cross-Zone Scripting Vulnerability
12228	Microsoft Windows Indexing Service Buffer Overflow Vulnerability
12095	Microsoft Windows LoadImage API Function Integer Overflow Vulnerability

January 10, 2005

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 13 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
12077	HP-UX FTP Server Debug Logging Mode Buffer Overflow Vulnerability
12098	HP-UX System Administration Manager Privilege Escalation Vulnerability
12061	IBM AIX CHCOD Local Privilege Escalation Vulnerability
12060	IBM AIX LSVPD Local Privilege Escalation Vulnerability
12160	Microsoft Internet Explorer FTP Client Directory Traversal Vulnerability
12124	Microsoft Internet Explorer Local File Disclosure Weakness
12094	Microsoft Windows ANI File Denial of Service Attack
12095	Microsoft Windows LoadImage API Function Integer Overflow Vulnerability
12092	Microsoft Windows winhlp32 Phrase Heap Overflow Vulnerability
12091	Microsoft Windows winhlp32 Phrase Integer Overflow Vulnerability
12057	Microsoft Windows XP Firewall ACL Bypass Vulnerability
12131	Mozilla Browser Network News Transport Protocol Remote Heap Overflow Vulnerability
12153	Mozilla/Firefox File Download Dialog Spoofing Vulnerability

December 22, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 8 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
12029	HP-UX Unspecified newgrp Local Privilege Escalation Vulnerability
12041	IBM AIX Diag Local Privilege Escalation Vulnerability

Bugtraq ID	Title
12043	IBM AIX PAGINITLocal Buffer Overflow Vulnerability
11950	Microsoft Internet Explorer DHTML Edit Control Script Injection Vulnerability
11883	Opera Web Browser Download Dialogue Box File Name Spoofing Vulnerability
11901	Opera Web Browser KDE KFMCLIENT Remote Command Execution Vulnerability
12032	Windows Media Player ActiveX Control File Enumeration Weakness
12031	Windows Media Player ActiveX Control Media File Attribute Corruption Weakness

December 15, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 29 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
11801	IBM AIX Multiple Local Vulnerabilities
11916	Hillgraave Hyper Terminal Session Data Buffer Overflow Vulnerability
11770	Microsoft Internet Explorer Drag and Drop Vulnerability
11826	Microsoft Internet Explorer FTP URI Arbitrary FTP Server Command Execution Vulnerability
11768	Microsoft Internet Explorer Image Download Filename Extension Spoofing Vulnerability
11751	Microsoft Internet Explorer Infinite Array Sort Denial Of Service Vulnerability
11855	Microsoft Internet Explorer Remote Window Hijacking Vulnerability
11851	Microsoft Internet Explorer Search Pane URI Obfuscation Vulnerability
11834	Microsoft Internet Explorer Sysimage Protocol Handler Local File Detection Vulnerability

Bugtraq ID	Title
11919	Microsoft Windows DHCP Server Logging Remote Denial Of Service Vulnerability
11920	Microsoft Windows DHCP Server Remote Buffer Overflow Vulnerability
11913	Microsoft Windows Kernel Unchecked LPC Buffer Privilege Escalation Vulnerability
11914	Microsoft Windows LSASS Connection Validation Privilege Escalation Vulnerability
11867	Microsoft Windows Multiple Unspecified Vulnerabilities
11769	Microsoft Windows WINS Arbitrary Association Delete Unspecified Buffer Overflow Vulnerability
11922	Microsoft Windows WINS Name Value Handling Remote Buffer Overflow Vulnerability
11763	Microsoft Windows WINS Replication Protocol Remote Memory Corruption Vulnerability
11929	Microsoft Word for Windows 6.0 Converter Font Conversion Buffer Overflow Vulnerability
11927	Microsoft Word for Windows 6.0 Converter Table Conversion Buffer Overflow Vulnerability
11854	Mozilla Browser and Mozilla Firefox Remote Window Hijacking Vulnerability
11760	Mozilla Browser Infinite Array Sort Denial Of Service Vulnerability
11752	Mozilla Firefox Infinite Array Sort Denial Of Service Vulnerability
11823	Mozilla/Netscape/Firefox Browsers JavaScript IFRAME Rendering Denial Of Service Vulnerability
11852	Netscape Remote Window Hijacking Vulnerability
11781	OpenSSH-portable PAM Authentication Remote Information Disclosure Vulnerability
11762	Opera Web Browser Infinite Array Sort Denial Of Service Vulnerability
11856	Opera Web Browser Remote Window Hijacking Vulnerability
11840	Sun Solaris IN.RWHOD(1M) Daemon Remote Code Execution Vulnerability
11782	Sun Solaris Ping Local Buffer Overflow Vulnerability

December 2, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 1 updated vulnerability.

Updated vulnerability

The following table includes information about the 1 updated vulnerability.

Bugtraq ID	Title
11515	Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability

November 30, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 18 additional vulnerabilities. The following table includes information about the vulnerabilities

Bugtraq ID	Title
6665	Kodak KCMS KCS_OPEN_PROFILE Procedure Arbitrary File Access Vulnerability
11680	Microsoft Internet Explorer Cookie Overwrite Vulnerability
11686	Microsoft Internet Explorer File Download Security Warning Bypass Vulnerability
11711	Microsoft Windows Logon Screensaver Local Privilege Escalation Vulnerability
10448	MIT Kerberos 5 KRB5_AName_To_Localname Multiple Principal Name Buffer Overrun Vulnerabilities
7184	MIT Kerberos 5 Principal Name Buffer Overflow Vulnerability
7185	MIT Kerberos 5 Principal Name Buffer Underrun Vulnerability
11712	Opera Web Browser Java Implementation Multiple Remote Vulnerabilities
11678	Samba QFILEPATHINFO Unicode Filename Remote Buffer Overflow Vulnerability
2605	Solaris kcms_configure KCMS_PROFILES Buffer Overflow Vulnerability

Bugtraq ID	Title
2475	Solaris tip Buffer Overflow Vulnerability
6279	Sun Solaris MailTool Attachment Denial Of Service Vulnerability
10261	Sun Solaris Patch Information Disclosure Vulnerability
10606	Sun Solaris Patches 112908-12 And 115168-03 Clear Text Password Logging Vulnerability
5268	Sun Solaris PCMCIA File Corruption Vulnerability
5208	Sun Solaris pkgadd Inappropriate File Permissions Vulnerability
5479	Sun XView Library Buffer Overflow Vulnerability
6016	YPServ Remote Network Information Leakage Vulnerability

November 16, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 18 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
11637	Microsoft Internet Explorer Embedded Content Status Bar URI Obfuscation Weakness
11565	Microsoft Internet Explorer HTML Form Malformed A Tag Status Bar Weakness
11590	Microsoft Internet Explorer IFRAME Status Bar URI Obfuscation Weakness
11621	Microsoft Internet Explorer Local Resource Enumeration Vulnerability
11561	Microsoft Internet Explorer TABLE Status Bar URI Obfuscation Weakness
11638	Microsoft Windows DDEShare Buffer Overflow Vulnerability
11643	Mozilla Firefox Download Dialogue Box File Name Spoofing Vulnerability
11644	Mozilla Firefox Insecure Default Installation Vulnerability
11648	Multiple Browser IMG Tag Multiple Vulnerabilities
11558	Multiple Vendor Content Filtering Bypass Vulnerabilities
11655	Multiple Vendor Server Response Filtering Weakness

Bugtraq ID	Title
11555	RealNetworks RealOne Player/RealPlayer Skin File Remote Stack Based Buffer Overflow Vulnerability
3457	Solaris in.fingerd Information Disclosure Vulnerability
5986	Solaris NFS lockd Remote Denial of Service Vulnerability
8305	Sun Solaris Runtime Linker LD_PRELOAD Local Buffer Overflow Vulnerability
6061	Sun Solaris Web-Based Enterprise Management Insecure Default File Permissions Vulnerability
5190	Sun Solaris in.dhcpd Malformed BOOTP Packet Buffer Overflow Vulnerability
2006	Unix Shell Redirection Race Condition Vulnerability

November 9, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 1 additional vulnerability. The following table includes information about the vulnerability.

Bugtraq ID	Title
11605	Microsoft ISA and Proxy Server Web Site Spoofing Vulnerability

November 2, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 19 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
11471	Apache mod_include Local Buffer Overflow Vulnerability
11412	Microsoft Frontpage Asycpict.DLL JPEG Handling Remote Denial of Service Vulnerabilities
11536	Microsoft Internet Explorer Font Tag Denial Of Service Vulnerability

Bugtraq ID	Title
11521	Microsoft Internet Explorer HHCtrl ActiveX Control Cross-Domain Scripting Vulnerability
11467	Microsoft Internet Explorer HTML Help Control Local Zone Security Restriction Bypass Vulnerability
11510	Microsoft Internet Explorer Malformed HTML Null Pointer Dereference Vulnerability
11515	Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability
11466	Microsoft Internet Explorer Valid File Drag and Drop Embedded Code Vulnerability
11446	Microsoft Outlook 2003 Security Policy Bypass Vulnerability
11447	Microsoft Outlook Express Plaintext Email Security Policy Bypass Vulnerability
11503	Microsoft Windows XP WAV File Handler Denial Of Service Vulnerability
11473	Mozilla Browser Cross-Domain Dialog Box Spoofing Vulnerability
11474	Mozilla Browser Cross-Domain Tab Window Form Field Focus Vulnerability
11440	Mozilla Invalid Pointer Dereference Vulnerability
11439	Mozilla Multiple Memory Corruption Vulnerabilities
11522	Mozilla Temporary File Insecure Permissions Information Disclosure Vulnerability
11441	Opera Browser TBODY COL SPAN Memory Corruption Denial Of Service Vulnerability
11475	Opera Web Browser Cross-Domain Dialog Box Spoofing Vulnerability
11459	Sun Solaris LDAP RBAC Local Privilege Escalation Vulnerability

October 18, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 14 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
11360	Apache mod_ssl SSLCipherSuite Access Validation Vulnerability
11342	Microsoft ASP.NET URI Canonicalization Remote Information Disclosure Vulnerability
11345	Microsoft Internet Explorer Local XML Document Disclosure Vulnerability
11388	Microsoft Internet Explorer Unspecified showHelp Zone Bypass Vulnerability
11387	Microsoft Windows 2003 Services Default Discretionary Access Controls Vulnerability
11410	Microsoft Windows XP Weak Default Configuration Vulnerability
11350	Microsoft Word Multiple Remote Denial Of Service Vulnerabilities
11311	Mozilla Firefox DATA URI File Deletion Vulnerability
11293	OpenSSL Unspecified Insecure Temporary File Creation Vulnerability
11309	RealNetworks RealOne Player And RealPlayer P Nen3260.DLL Remote Integer Overflow Vulnerability
11308	RealNetworks RealOne Player And RealPlayer Unspecified File Deletion Vulnerability
11307	RealNetworks RealOne Player And RealPlayer Unspecified Web Page Code Execution Vulnerability
11335	RealOne Player and RealPlayer Multiple Unspecified Remote Vulnerabilities
11318	Sun Solaris Gzip File Permission Modification Vulnerability

October 12, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 16 additional vulnerabilities and 6 updated vulnerabilities. The following tables include information about the vulnerabilities.

Bugtraq ID	Title
11373	Microsoft Excel File Handler Unspecified Buffer Overflow Vulnerability
11384	Microsoft IIS Server WebDAV XML Requests Denial of Service Vulnerability
11377	Microsoft Internet Explorer Double Byte Character Set Handling Address Bar Spoofing Vulnerability
11367	Microsoft Internet Explorer Heartbeat ActiveX Control Unspecified Vulnerability
11366	Microsoft Internet Explorer Install Engine ActiveX Control Buffer Overflow Vulnerability
11381	Microsoft Internet Explorer Plug-in Navigations Handling Address Bar Spoofing Vulnerability
11383	Microsoft Internet Explorer Secure Sockets Layer Caching Vulnerability
11379	Microsoft NNTP Component Buffer Overflow Vulnerability
11380	Microsoft RPC Runtime Library Remote Denial Of Service And Information Disclosure Vulnerability
11374	Microsoft SMTP Service and Exchange Routing Engine Buffer Overflow Vulnerability
11378	Microsoft Window Management API Local Privilege Escalation Vulnerability
11382	Microsoft Windows Compressed (zipped) Folder Buffer Overflow Vulnerability
11365	Microsoft Windows Kernel Local Denial of Service Vulnerability
11369	Microsoft Windows Kernel Virtual DOS Machine Privilege Escalation Vulnerability
11372	Microsoft Windows NetDDE Remote Buffer Overflow Vulnerability
11375	Microsoft Windows WMF/EMF Image Format Rendering Remote Buffer Overflow Vulnerability

Updated vulnerabilities

The following table includes information about 6 updated vulnerabilities.

Bugtraq ID	Title
10973	Microsoft Internet Explorer Implicit Drag and Drop File Installation Vulnerability
10689	Microsoft Internet Explorer JavaScript Method Assignment Cross-Domain Scripting Vulnerability
10690	Microsoft Internet Explorer Popup.show Mouse Event Hijacking Vulnerability
10816	Microsoft Internet Explorer Style Tag Comment Memory Corruption Vulnerability
10677	Microsoft Windows Program Group Converter Filename Local Buffer Overrun Vulnerability
10213	Microsoft Windows Shell Long Share Name Buffer Overrun Vulnerability

October 6, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 8 additional vulnerabilities. The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
11239	Apache Satisfy Directive Access Control Bypass Vulnerability
11264	IBM CTSTRTCASD Utility Local File Corruption Vulnerability
11251	Microsoft GDI+ Library Malformed JPEG Handling Unspecified Denial of Service Vulnerability
11265	Microsoft SQL Server Remote Denial Of Service Vulnerability
11258	Multiple Vendor TCP Packet Fragmentation Handling Denial Of Service Vulnerability
11273	RealNetworks RealOne Player And RealPlayer Remote Vulnerabilities
11281	Samba Remote Arbitrary File Access Vulnerability
11216	Samba Samba-VScan Undisclosed Denial Of Service Vulnerability

September 21, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 19 additional vulnerabilities. The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
11185	Apache Mod_DAV LOCK Denial Of Service Vulnerability
11182	Apache Web Server Configuration File Environment Variable Local Buffer Overflow Vulnerability
11187	Apache Web Server Remote IPv6 Buffer Overflow Vulnerability
11094	Apache mod_ssl Denial Of Service Vulnerability
11154	Apache mod_ssl Remote Denial of Service Vulnerability
11200	Microsoft Internet Explorer User Security Confirmation Bypass Vulnerability
11202	Microsoft Windows XP Explorer.EXE TIFF Image Denial of Service Vulnerability
11171	Mozilla Browser BMP Image Decoding Multiple Integer Overflow Vulnerabilities
11169	Mozilla Browser Non-ASCII Hostname Heap Overflow Vulnerability
11174	Mozilla Browser Vcard Handling Remote Buffer Overflow Vulnerability
11166	Mozilla Firefox Default Installation File Permission Vulnerability
11170	Mozilla Multiple URI Processing Heap Based Buffer Overflow Vulnerabilities
11177	Mozilla/Firefox Browsers URI Drag And Drop Cross-Domain Scripting Vulnerability
11179	Mozilla/Firefox Browsers Unauthorized Clipboard Contents Disclosure Vulnerability
11192	Mozilla/Firefox Browsers Tar.GZ Archive Weak Permission Vulnerability
11194	Mozilla/Firefox Browsers PrivilegeManager EnablePrivilege Dialog Manipulation Vulnerability
11186	Multiple Browser Cross-Domain Cookie Injection Vulnerability
11156	Samba Multiple ASN.1 and MailSlot Parsing Remote Denial Of Service Vulnerabilities

Bugtraq ID	Title
11118	Sun Solaris in.named Remote Denial of Service Vulnerability

September 14, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 2 additional vulnerabilities. The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
11172	Microsoft WordPerfect Converter Remote Buffer Overflow Vulnerability
11173	Microsoft GDI+ Library JPEG Segment Length Integer Underflow Vulnerability

September 7, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 11 additional vulnerabilities. The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
11050	CDE LibDTHelp LOGNAME Environment Variable Local Buffer Overflow Vulnerability
10973	Microsoft Internet Explorer Drag And Drop File Installation Vulnerability
10979	Microsoft Internet Explorer MHTML IMG Source Attribute Cross Security Domain Scripting Vulnerability
11026	Microsoft Internet Explorer Resource Detection Weakness
10980	Microsoft NTP Time Synchronization Spoof Weakness
11040	Microsoft Outlook Express BCC Field Information Disclosure Vulnerability
11090	Opera Web Browser Empty Embedded Object JavaScript Denial Of Service Vulnerability
10997	Opera Web Browser JavaScript Denial Of Service Vulnerability
10961	Opera Web Browser Resource Detection Weakness

Bugtraq ID	Title
11055	Samba Remote Print Change Notify Denial Of Service Vulnerability
11027	Sun DtMail Local Command Line Format String Vulnerability

August 18, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 46 additional vulnerabilities. The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
10244	LibPNG Broken PNG Out Of Bounds Access Denial Of Service Vulnerability
6431	LibPNG Incorrect Offset Calculation Buffer Overflow Vulnerability
5059	LibPNG Malformed PNG Image Memory Corruption Vulnerability
10879	Microsoft Internet Explorer mms Protocol Handler Executable Command Line Injection Vulnerability
10943	Microsoft Internet Explorer Spoofed Address Bar Vulnerability
10901	Microsoft Windows 2000/XP CRL File Failed Integrity Check Denial Of Service Vulnerability
10930	Microsoft Windows Internet Connection Firewall Filter Bypass Vulnerability
10897	Microsoft Windows XP SP2 Released - Multiple Vulnerabilities Fixed
4628	Mozilla / Netscape 6 XMLHttpRequest File Disclosure Vulnerability
10843	Mozilla and Netscape SOAPParameter Integer Overflow Vulnerability
10874	Mozilla Browser Input Type HTML Tag Unauthorized Access Vulnerability
10876	Mozilla Browser Non-FQDN SSL Certificate Spoofing Vulnerability
10875	Mozilla Browser/Thunderbird SendUIDL POP3 Message Handling Remote Heap Overflow Vulnerability
10877	Mozilla Cross-Domain Frame Loading Vulnerability
10880	Mozilla SSL Redirect Spoofing Vulnerability
5002	Netscape / Mozilla Malformed Email POP3 Denial Of Service Vulnerability

Bugtraq ID	Title
8180	Netscape Client Detection Tool Plug-In Buffer Overflow Vulnerability
618	Netscape Communicator EMBED Buffer Overflow Vulnerability
1260	Netscape Communicator Inconsistent SSL Certificate Warning Vulnerability
1120	Netscape Communicator Javascript-in-Cookies Vulnerability
822	Netscape Communicator Long Argument Vulnerability
6981	Netscape Communicator Password Disclosure Weakness
1726	Netscape Communicator type=password Browser Buffer Overflow Vulnerability
5010	Netscape Composer Font Face Field Buffer Overflow Vulnerability
500	Netscape core file Vulnerability
2824	Netscape 'document.referrer' User Information Disclosure Vulnerability
6499	Netscape Email Client Message Deletion Weakness
6256	Netscape Java canConvert() Buffer Overflow Vulnerability
6223	Netscape Java Virtual Machine Insecure Call Vulnerability
6796	Netscape JavaScript Cache Browsing Vulnerability
6959	Netscape JavaScript Regular Expression Denial Of Service Vulnerability
2637	Netscape Navigator 'about:' Domain Information Disclosure Vulnerability
1188	Netscape Navigator and Communicator Invalid SSL Certificate Warning Bypass Vulnerability
7456	Netscape Navigator Directory Cross-Domain Scripting Vulnerability
10389	Netscape Navigator Embedded Image URI Obfuscation Weakness
7564	Netscape Navigator False URL Information Vulnerability
6937	Netscape Style Sheet Denial Of Service Vulnerability
6215	Netscape User Preferences Information Disclosure Vulnerability
4637	Netscape/Mozilla IRC Buffer Overflow Vulnerability
6185	Netscape/Mozilla JAR Remote Heap Corruption Vulnerability
3925	Netscape/Mozilla Null Character Cookie Stealing Vulnerability

Bugtraq ID	Title
6254	Netscape/Mozilla POP3 Mail Handler Integer Overflow Vulnerability
4640	Netscape/Mozilla/Galeon Local File Detection Vulnerability
10873	Opera Remote Location Object Cross-Domain Scripting Vulnerability
10934	RealNetwork RealPlayer Unspecified Remote Vulnerability
10911	Sun Solaris XDMCP Unspecified Denial Of Service Vulnerability

August 10, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 12 additional vulnerabilities and 7 updated vulnerabilities. The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
10789	Apache mod_userdir Module Information Disclosure Vulnerability
10857	LibPNG Graphics Library Multiple Remote Vulnerabilities
10902	Microsoft Exchange Outlook Web Access Script Injection Vulnerability
10816	Microsoft Internet Explorer Style Tag Comment Memory Corruption Vulnerability
10709	Mozilla Browser Cache File Multiple Vulnerabilities
9329	Mozilla Firebird Browser markLinkVisited Arbitrary Script Code Execution Vulnerability
10796	Mozilla Firefox Refresh Security Property Spoofing Vulnerability
10832	Mozilla Firefox XML User Interface Language Browser Interface Spoofing Vulnerability
7847	Multiple Browser Timed Document.Write Method Cross Domain Policy Vulnerability
5665	Multiple Browser Zero Width GIF Image Memory Corruption Vulnerability
10810	Opera Web Browser Location Replace URI Obfuscation Weakness
10809	Sun Solaris 'ypbind' Unspecified Buffer Overflow Vulnerability

Updated vulnerabilities

The following table includes information about the 7 updated vulnerabilities.

Bugtraq ID	Title
7363	Mozilla Browser Cross Domain Violation Vulnerability
10532	Mozilla Browser URI Obfuscation Weakness
10681	Mozilla External Protocol Handler Weakness
5346	Multiple Browser Vendor Same Origin Policy Design Error Vulnerability
10661	Multiple Vendor Internet Browser User Action Prediction/Interception Weakness
10341	Multiple Vendor URI Protocol Handler Arbitrary File Creation/Modification Vulnerability
7227	Multiple Vendor Web Browser LiveConnect JavaScript Denial Of Service Vulnerability

July 30, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 3 additional vulnerabilities. The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
9663	Microsoft Internet Explorer Bitmap Processing Integer Overflow Vulnerability
8530	Microsoft Internet Explorer Malformed GIF Double Free Code Execution Vulnerability
10473	Microsoft Internet Explorer Modal Dialog Zone Bypass Vulnerability

July 27, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 42 additional vulnerabilities and reports 15 updated vulnerabilities.

Note: Windows Server 2003 agents have added detection of 338 vulnerabilities.

The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
10689	Microsoft Internet Explorer JavaScript Function Assignment Cross-Domain Scripting Vulnerability
10694	Microsoft Internet Explorer JavaScript Null Pointer Exception Denial Of Service Vulnerability
10690	Microsoft Internet Explorer Popup.show Mouse Event Hijacking Vulnerability
8244	Microsoft Multiple IIS 6.0 Web Admin Vulnerabilities
10692	Microsoft Outlook Express Message Window Script Execution Vulnerability
10693	Microsoft Windows 2000 Media Player Control Media Preview Script Execution Vulnerability
10683	Microsoft Word/Outlook Object Tag Security Setting Compromise Vulnerability
9323	Mozilla Browser Cookie Path Restriction Bypass Vulnerability
7363	Mozilla Browser Cross Domain Violation Vulnerability
9328	Mozilla Browser Custom Getter/Setter Objects Same Origin Policy Violation Vulnerability
9324	Mozilla Browser Default HTA Handling Weakness
9326	Mozilla Browser Proxy Server Authentication Credential Disclosure Vulnerability
9325	Mozilla Browser Scope Cross-Domain Function Or Variable Disclosure Vulnerability
9322	Mozilla Browser Script.prototype.freeze/thaw Arbitrary Code Execution Vulnerability
9203	Mozilla Browser URI MouseOver Obfuscation Weakness
10532	Mozilla Browser URI Obfuscation Weakness
10681	Mozilla External Protocol Handler Weakness
5293	Mozilla JavaScript URL Host Spoofing Arbitrary Cookie Access Vulnerability

10694	Microsoft Internet Explorer JavaScript Null Pointer Exception Denial Of Service Vulnerability
10690	Microsoft Internet Explorer Popup.show Mouse Event Hijacking Vulnerability
8244	Microsoft Multiple IIS 6.0 Web Admin Vulnerabilities
10692	Microsoft Outlook Express Message Window Script Execution Vulnerability
10693	Microsoft Windows 2000 Media Player Control Media Preview Script Execution Vulnerability
10683	Microsoft Word/Outlook Object Tag Security Setting Compromise Vulnerability
9323	Mozilla Browser Cookie Path Restriction Bypass Vulnerability
7363	Mozilla Browser Cross Domain Violation Vulnerability
9328	Mozilla Browser Custom Getter/Setter Objects Same Origin Policy Violation Vulnerability
9324	Mozilla Browser Default HTA Handling Weakness
9326	Mozilla Browser Proxy Server Authentication Credential Disclosure Vulnerability
9325	Mozilla Browser Scope Cross-Domain Function Or Variable Disclosure Vulnerability
9322	Mozilla Browser Script.prototype.freeze/thaw Arbitrary Code Execution Vulnerability
9203	Mozilla Browser URI MouseOver Obfuscation Weakness
10532	Mozilla Browser URI Obfuscation Weakness
10681	Mozilla External Protocol Handler Weakness
5293	Mozilla JavaScript URL Host Spoofing Arbitrary Cookie Access Vulnerability

Bugtraq ID	Title
9579	Multiple RealPlayer/RealOne Player Supported File Type Buffer Overrun Vulnerabilities
6361	Multiple Unspecified RealOne Player Buffer Overflow Vulnerabilities
10661	Multiple Vendor Internet Browser User Action Prediction/Interception Weakness
7227	Multiple Vendor Web Browser LiveConnect JavaScript Denial Of Service Vulnerability
10763	Opera Web Browser Cross-Domain Frame Loading Vulnerability
10679	Opera Web Browser IFrame OnLoad Address Bar URL Obfuscation Weakness
10764	Opera Web Browser Unspecified Certificate Verification Vulnerability
1088	Real Networks RealPlayer 6/7 Location Buffer Overflow Vulnerability
4221	Real Networks RealPlayer Directory Traversal Vulnerability
4200	Real Networks Realplayer 8 CPU Utilization Denial of Service Vulnerability
10528	RealNetwork RealPlayer EMBD3260.DLL Error Response Heap Overflow Vulnerability
10520	RealNetwork RealPlayer Media File Heap Overflow Vulnerabilities
10527	RealNetworks RealPlayer URI Processing Buffer Overrun Vulnerability
9378	RealOne Player SMIL File Script Execution Variant Vulnerability
8839	RealOne Player Temporary File Default Browser Script Execution Vulnerability
9580	RealPlayer/RealOne Player RMP Skin File Handler Directory Traversal Vulnerability
10781	Samba Filename Mangling Method Buffer Overrun Vulnerability
10780	Samba Web Administration Tool Base64 Decoder Buffer Overflow Vulnerability
1200	Solaris netpr Buffer Overflow Vulnerability
10747	Sun Solaris Volume Manager Denial Of Service Vulnerability

Updated vulnerabilities

The following table includes information about the 15 updated vulnerabilities.

Bugtraq ID	Title
5757	Mozilla Browser HTTP/HTTPS Redirection Weakness
5753	Mozilla Browser Large HTTP Header Buffer Overflow Vulnerability
9747	Mozilla Browser Zombie Document Cross-Site Scripting Vulnerability
5403	Mozilla FTP View Cross-Site Scripting Vulnerability
5741	Mozilla Netscape Navigator Plug-In Path Disclosure Vulnerability
5694	Mozilla OnUnload Referer Information Leakage Vulnerability
3743	Mozilla Predictable Temporary File Symbolic Link Attack Vulnerability
5762	Mozilla Space Key XPI Installation Vulnerability
5766	Mozilla XMLSerializer Same Origin Policy Violation Vulnerability
5759	Mozilla document.open() Memory Corruption Denial of Service Vulnerability
9182	Multiple Browser URI Display Obfuscation Weakness
5346	Multiple Browser Vendor Same Origin Policy Design Error Vulnerability
3684	Multiple Vendor Image Count Denial of Service Vulnerability
4322	Multiple Vendor JavaScript Interpreter Denial Of Service Vulnerability
5742	Netscape/Mozilla Javascript Array Object Heap Corruption Vulnerability

July 13, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 9 additional vulnerabilities and reports 2 updated vulnerabilities. The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
10594	Sun Solaris Basic Security Module Auditing Denial Of Service Vulnerability
10627	Microsoft Internet Explorer Cross-Domain Frame Loading Vulnerability

Bugtraq ID	Title
10652	Microsoft Internet Explorer Shell.Application Object Script Execution Weakness
10705	Microsoft Windows HTML Help Heap Overflow Vulnerability
10706	Microsoft IIS 4 Redirect Remote Buffer Overflow Vulnerability
10707	Microsoft Windows Utility Manager Local Privilege Escalation Variant Vulnerability
10708	Microsoft Windows Task Scheduler Remote Buffer Overflow Vulnerability
10710	Microsoft Windows POSIX Subsystem Buffer Overflow Local Privilege Escalation Vulnerability
10711	Microsoft Outlook Express Malformed Email Header Denial Of Service Vulnerability

Updated vulnerabilities

The following table includes information about the 2 updated vulnerabilities.

Bugtraq ID	Title
9320	Microsoft Internet Explorer showHelp CHM File Execution Weakness
9510	Microsoft Internet Explorer CLSID File Extension Misrepresentation Vulnerability

July 6, 2004

This content update for Symantec Vulnerability Assessment 1.0 reports 1 updated vulnerability. The following tables includes information about the vulnerability.

Bugtraq ID	Title
10514	Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness

June 29, 2004

This content update for Symantec Vulnerability Assessment 1.0 includes an engine update release 1.0.4 and detects and reports 13 additional vulnerabilities and reports 33 updated vulnerabilities. The following tables includes information about the vulnerabilities.

Bugtraq ID	Title
10551	HP-UX Local X Font Server Buffer Overflow Vulnerability
10292	Microsoft ASP.NET Malformed HTTP Request Information Disclosure Vulnerability
10579	Microsoft Internet Explorer Non-FQDN URI Address Zone Bypass Vulnerability
10514	Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness
10552	Microsoft Internet Explorer HREF Save As Denial of Service Vulnerability
10517	Microsoft Internet Explorer URI Obfuscation Weakness
10554	Microsoft Internet Explorer Wildcard DNS Cross-Site Scripting Vulnerability
4449	Microsoft Office Web Components Active Script Execution Vulnerability
4454	Microsoft Office Web Components Chart Local File Existence Disclosure Vulnerability
4457	Microsoft Office Web Components Clipboard Information Disclosure Vulnerability
4453	Microsoft Office Web Components Local File Read Vulnerability
4456	Microsoft OWC DataSourceControl ConnectionFile Local File Existence Disclosure Vulnerability
4455	Microsoft OWC Spreadsheet XMLURL Local File Existence Disclosure Vulnerability

Updated vulnerabilities

Engine Update release 1.0.4 for Symantec Vulnerability Assessment 1.0 updates the SVA Manager so that audits can be run against Windows Server 2003

Agents. The following table includes information about the 33 updated Windows Server 2003 vulnerabilities.

Bugtraq ID	Title
8830	Microsoft ActiveX Authenticode Verification Bypass Vulnerability
10118	Microsoft ASN.1 Library Double Free Memory Corruption Vulnerability
9633	Microsoft ASN.1 Library Length Integer Mishandling Memory Corruption Vulnerability
9743	Microsoft ASN.1 Library Multiple Stack-Based Buffer Overflow Vulnerabilities
9118	Microsoft Exchange Server 2003 Outlook Web Access Lowered Security Settings Weakness
10112	Microsoft Jet Database Engine Remote Code Execution Vulnerability
8827	Microsoft ListBox/ComboBox Control User32.dll Function Buffer Overrun 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
7788	Microsoft Windows 2000/XP/2003 IPV6 ICMP Flood Denial Of Service Vulnerability
9635	Microsoft Windows ASN.1 Library Bit String Processing Integer Handling Vulnerability
10123	Microsoft Windows COM Internet Service/RPC Over HTTP Remote Denial Of Service Vulnerability
8205	Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability
7358	Microsoft Windows EngTextOut Non-ASCII Character Denial Of Service Vulnerability
7849	Microsoft Windows FIN-ACK Network Device Driver Frame Padding Information Disclosure Vulnerability
10111	Microsoft Windows H.323 Remote Buffer Overflow Vulnerability
8828	Microsoft Windows Help And Support Center URI Handler Buffer Overflow Vulnerability

Bugtraq ID	Title
10119	Microsoft Windows Help And Support Center URI Validation Code Execution Vulnerability
10321	Microsoft Windows HSC DVD Driver Upgrade Code Execution Vulnerability
8016	Microsoft Windows HTML Converter HR Align Buffer Overflow Vulnerability
9624	Microsoft Windows Internet Naming Service Buffer Overflow Vulnerability
10108	Microsoft Windows LSASS Buffer Overrun Vulnerability
8783	Microsoft Windows Message Queuing Service Heap Overflow Vulnerability
8826	Microsoft Windows Messenger Service Buffer Overrun Vulnerability
8532	Microsoft Windows NetBIOS Name Service Reply Information Leakage Weakness
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
10115	Microsoft Windows SSL Library Denial of Service Vulnerability
8522	Multiple Microsoft Windows 2003 Stack Protection Implementation Weaknesses

June 15, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 9 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
10473	Microsoft Internet Explorer Modal Dialog Zone Bypass Vulnerability
10472	Microsoft Internet Explorer URL Local Resource Access Weakness
10484	Microsoft ISA Server 2000 FTP Bounce Filtering Vulnerability

Bugtraq ID	Title
10480	Microsoft ISA Server 2000 Site And Content Rule Bypass Vulnerability
10481	Microsoft ISA Server HTTP Authentication Scheme Vulnerability
10482	Microsoft ISA Server Redirect URI Handler Web Proxy Service Remote Denial Of Service Vulnerability
10477	Microsoft ISA Server Web Proxy Malformed SSL Packet Remote Denial of Service Vulnerability
10440	Microsoft Windows 2000 Domain Expired Account Security Policy Violation Weakness
10452	Opera Browser Favicon Address Bar Spoofing Weakness

June 8, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 2 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
10260	Business Objects Crystal Reports Web Form Viewer Directory Traversal Vulnerability
10487	Microsoft DirectX DirectPlay Remote Malformed Packet Denial Of Service Vulnerability

June 1, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 15 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
10355	Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability
10344	Microsoft Internet Explorer Codebase Double Backslash Local Zone File Execution Weakness

Bugtraq ID	Title
10382	Microsoft Internet Explorer CSS Style Sheet Memory Corruption Vulnerability
10348	Microsoft Internet Explorer Double Backslash CHM File Execution Weakness
10351	Microsoft Internet Explorer http-equiv Meta Tag Denial of Service Vulnerability
10346	Microsoft Internet Explorer Interface Spoofing Vulnerability
10318	Microsoft Internet Explorer XML Parsing Denial Of Service Vulnerability
10324	Multiple Mail Transfer Agent Embedded Hyperlink URI Obfuscation Variant Weakness
10369	Microsoft Outlook 2003 Media File Script Execution Vulnerability
10345	Microsoft Outlook Express URI Obfuscation Vulnerability
10323	Microsoft Outlook Mail Client E-mail Address Verification Weakness
10363	Microsoft Windows XP Self-Executing Folder Vulnerability
10337	Opera Web Browser Address Bar Spoofing Weakness
10341	Opera Web Browser Telnet URI handler Arbitrary File Creation/Modification Vulnerability
10349	Sun Solaris Management Console Information Disclosure Vulnerability

May 18, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 10 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
9905	AIX Getlvcb Command Line Argument Buffer Overflow Vulnerability
9906	AIX Putlvcb Command Line Argument Buffer Overflow Vulnerability
9958	Common Desktop Environment DTLogin Unspecified Remote Double Free Vulnerability
5064	Microsoft Excel Drawing Shape Hyperlink Macro Execution Vulnerability

Bugtraq ID	Title
5063	Microsoft Excel Embedded Object Inline Macro Execution Vulnerability
4821	Microsoft Excel XML Stylesheet Arbitrary Code Execution Vulnerability
10308	Microsoft Internet Explorer Embedded Image URI Obfuscation Weakness
10299	Microsoft Internet Explorer Unconfirmed Memory Corruption Vulnerability
10307	Microsoft Outlook 2003 Predictable File Location Weakness
4397	Microsoft Outlook HTML Mail Script Execution Vulnerability

May 11, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 1 additional vulnerability. The following table includes information about the vulnerability.

Bugtraq ID	Title
10321	Microsoft Windows HSC DVD Driver Upgrade Code Execution Vulnerability

May 4, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 30 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
10212	Apache mod_auth Malformed Password Potential Memory Corruption Vulnerability
7796	HP-UX UUCP Unspecified Buffer Overflow Vulnerability
6214	Microsoft Data Access Components RDS Buffer Overflow Vulnerability
7735	Microsoft IIS WebDAV PROPFIND and SEARCH Method Denial of Service Vulnerability
6205	Microsoft Internet Explorer IFRAME dialogArguments Cross-Zone Access Vulnerability

Buqtraq ID	Title
10248	Microsoft Internet Explorer Meta Data Foreign Domain Spoofing Vulnerability
10167	Microsoft Internet Explorer Object Element Data Denial Of Service Vulnerability
8034	Microsoft Media Player 9 Unauthorized Media Library Access Vulnerability
10213	Microsoft Windows Long Share Name Buffer Overrun Vulnerability
3156	Microsoft Windows Media Player .ASF Marker Buffer Overflow Vulnerability
1980	Microsoft Windows Media Player .ASX Buffer Overflow Vulnerability
3105	Microsoft Windows Media Player .NSC File Buffer Overflow Vulnerability
1976	Microsoft Windows Media Player .WMS Arbitrary Script Vulnerability
2203	Microsoft Windows Media Player .WMZ Arbitrary Java Applet Vulnerability
1714	Microsoft Windows Media Player 7 Embedded OCX Control Vulnerability
5543	Microsoft Windows Media Player File Attachment Script Execution Vulnerability
5357	Microsoft Windows Media Player Filename Buffer Overflow Vulnerability
2167	Microsoft Windows Media Player Javascript URL Vulnerability
7517	Microsoft Windows Media Player Skin File Code Execution Vulnerability
10231	Multiple IBM AIX Unspecified Console Commands Symbolic Link Vulnerabilities
10230	Multiple IBM AIX Unspecified LVM Utilities Symbolic Link Vulnerabilities
10202	Sun Solaris SendFileV Local Denial Of Service Vulnerability
10216	Sun Solaris TCP/IP Networking Stack Unspecified Denial of Service Vulnerability
2677	Windows Media Player .ASX Buffer Overflow Vulnerability
2686	Windows Media Player .ASX 'Version' Buffer Overflow Vulnerability
5107	Windows Media Player IE Cache Path Disclosure Vulnerability
2765	Windows Media Player Internet Shortcut Execution Vulnerability
5110	Windows Media Player Playlist HTML Script Execution Vulnerability
5109	Windows Media Player WMDM Privilege Escalation Vulnerability

Buqtraq ID	Title
10199	Yahoo! Messenger YInsthelper.DLL Multiple Buffer Overflow Vulnerabilities

April 20, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 24 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugraq ID	Title
7539	Internet Explorer file:// Request Zone Bypass Vulnerability
10073	Internet Explorer Remote IFRAME Denial Of Service Vulnerability
10097	Microsoft Internet Explorer Bitmap File Processing Denial of Service Vulnerability
3513	Microsoft Internet Explorer Cookie Disclosure/Modification Vulnerability
5561	Microsoft Internet Explorer Dialog Same Origin Policy Bypass Variant Vulnerability
6306	Microsoft Internet Explorer Dialog Style Same Origin Policy Bypass Vulnerability
6749	Microsoft Internet Explorer dragDrop Method Local File Reading Vulnerability
5558	Microsoft Internet Explorer Legacy Text Formatting ActiveX Component Buffer Overflow Vulnerability
10056	Microsoft Internet Explorer MSWebDVD Object Denial of Service Vulnerability
7806	Microsoft Internet Explorer OBJECT Tag Buffer Overflow Vulnerability
5196	Microsoft Internet Explorer OBJECT Tag Same Origin Policy Violation Vulnerability
7419	Microsoft Internet Explorer Remote URLMON.DLL Buffer Overflow Vulnerability
5560	Microsoft Internet Explorer XML Redirect File Disclosure Vulnerability
10098	Microsoft Outlook Express Malformed EML File Denial of Service Vulnerability

Bugtraq ID	Title
10144	Microsoft Outlook/Outlook Express Remote Denial Of Service Vulnerability
5557	Multiple Microsoft Internet Explorer Vulnerabilities
4930	Multiple Microsoft Product Gopher Client Buffer Overflow Vulnerability
5356	Multiple Vendor Sun RPC xdr_array Buffer Overflow Vulnerability
9986	OpenSSH SCP Client File Corruption Vulnerability
9899	OpenSSL Denial of Service Vulnerabilities
10081	Opera Web Browser Remote IFRAME Denial Of Service Vulnerability
8873	Sun Management Center Error Message Information Disclosure Vulnerability
10080	Sun Solaris Secure Shell Daemon Client Logging Weakness
9548	Sun Solaris TCSetAttr System Hang Denial Of Service Vulnerability

April 13, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports eighteen additional vulnerabilities and two updated vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
10108	Microsoft Windows LSASS Buffer Overrun Vulnerability
10111	Microsoft Windows H.323 Remote Buffer Overflow Vulnerability
10112	Microsoft Jet Database Engine Remote Code Execution Vulnerability
10113	Microsoft Negotiate SSP Remote Buffer Overflow Vulnerability
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

Bugtraq ID	Title
10119	Microsoft Windows Help And Support Center URI Validation Code Execution Vulnerability
10120	Microsoft Windows WMF/EMF Image Formats Remote Buffer Overflow Vulnerability
10121	Microsoft Windows Object Identity Network Communication Vulnerability
10122	Microsoft Windows Local Descriptor Table Local Privilege Escalation Vulnerability
10123	Microsoft Windows COM Internet Service And RPC over HTTP Remote Denial Of Service Vulnerability
10124	Microsoft Windows Utility Manager Local Privilege Escalation Vulnerability
10125	Microsoft Windows Management Local Privilege Escalation Vulnerability
10126	Microsoft Windows Logon Process Remote Buffer Overflow Vulnerability
10127	Microsoft Windows RPCSS Service Remote Denial Of Service

Updated vulnerabilities

The following table includes information about the two updated vulnerabilities.

Bugtraq ID	Title
8811	Microsoft Windows RPCSS Multi-thread Race Condition Vulnerability
9105	Outlook Express MHTML Forced File Execution Vulnerability

April 6, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 23 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
2916	AIX diagrpt Arbitrary Privileged Program Execution Vulnerability
9982	AIX Invscountd Symbolic Link Vulnerability

Bugtraq ID	Title
9921	Apache Connection Blocking Denial Of Service Vulnerability
9930	Apache Connection Blocking Denial Of Service Vulnerability
9874	Apache HTAccess LIMIT Directive Bypass Configuration Error Weakness
5925	IBM AIX Remote Empty TCP Flag Flood Denial Of Service Vulnerability
8536	Microsoft Access Snapshot Viewer ActiveX Control Parameter Buffer Overflow Vulnerability
9010	Microsoft Excel XLM Macro Security Level Bypass Vulnerability
5559	Microsoft Internet Explorer Download Dialogue File Source Obfuscation Vulnerability
10023	Microsoft Internet Explorer HTML Form Status Bar Misrepresentation Vulnerability
6923	Microsoft Outlook and Outlook Express Arbitrary Program Execution Vulnerability
5473	Microsoft Outlook Express MHTML URL Handler File Rendering Vulnerability
5944	Microsoft Outlook Express S/MIME Buffer Overflow Vulnerability
2297	Microsoft PowerPoint Buffer Overflow Vulnerability
2018	Microsoft Windows 2000 Telnet Session Timeout DoS Vulnerability
9924	Microsoft Windows XP Explorer.EXE Remote Denial of Service Vulnerability
8835	Microsoft Word Macro Name Handler Buffer Overflow Vulnerability
6821	Multiple Vendor Email Client JavaScript Information Leakage Vulnerability
8732	OpenSSL ASN.1 Parsing Vulnerabilities
9962	Sun Solaris vfs_getvfsw function Local Privilege Escalation Vulnerability
4408	Sun Solaris XSun Color Database File Heap Overflow Vulnerability
10003	TCPDump ISAKMP Delete Payload Buffer Overrun Vulnerability
10004	TCPDump ISAKMP Identification Payload Integer Underflow Vulnerability

March 23, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 52 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
1087	Microsoft Excel XML Vulnerability
1631	Microsoft Outlook Rich Text Format Information Disclosure Vulnerability
1633	Microsoft Outlook Vcard DoS Vulnerability
2260	Microsoft Outlook Concealed Attachment Vulnerability
2459	Microsoft Outlook vcard Buffer Overflow Vulnerability
2753	Microsoft Word RTF Template Macro Execution Vulnerability
2823	Microsoft Outlook Express Address Book Spoofing Vulnerability
3025	Microsoft Outlook Unauthorized Email Access Vulnerability
3026	Microsoft Outlook Arbitrary Code Execution Vulnerability
3334	Microsoft Outlook Express 6 Plain Text Message Script Execution Vulnerability
3722	Microsoft Excel Spreadsheet Data Password Protection Bypass Vulnerability
4028	Microsoft MSN ActiveX Object Information Disclosure Vulnerability
4092	Outlook Express Attachment Carriage Return/Linefeed Encapsulation Filtering Bypass Vulnerability
4316	Microsoft MSN Messenger Message Spoofing Vulnerability
4334	Microsoft Outlook IFrame Embedded URL Vulnerability
4337	Microsoft Outlook Javascript Execution Vulnerability
4340	Microsoft Outlook IFrame Embedded Media Player File Vulnerability
4341	Microsoft Outlook Disabled Cookies Setting Bypass Vulnerability
4398	Microsoft Office XP Spreadsheet Host().SaveAs() File Creation Vulnerability
4584	Microsoft Outlook Express DOS Device Denial of Service Vulnerability
4675	Microsoft MSN Messenger Font Tag Denial Of Service Vulnerability
4827	Microsoft MSN Messenger Malformed Invite Request Denial of Service

Bugtraq ID	Title
5274	Microsoft Outlook Express SMTP Over TLS Information Disclosure Vulnerability
5277	Microsoft Outlook Express Spoofable File Extensions Vulnerability
5350	Microsoft Outlook Express XML File Attachment Script Execution Vulnerability
5420	Microsoft Content Management Server 2001 User Authentication Buffer Overflow Vulnerability
5421	Microsoft Content Management Server 2001 Arbitrary Upload Location Vulnerability
5422	Microsoft Content Management Server 2001 SQL Injection Vulnerability
5682	Alleged Outlook Express Link Denial of Service Vulnerability
5764	Microsoft Word INCLUDEPICTURE Document Sharing File Disclosure Vulnerability
5922	Microsoft Content Management Server 2001 Cross-Site Scripting Vulnerability
6319	Microsoft Outlook 2002 Email Header Processing Denial of Service Vulnerability
6667	Microsoft Outlook 2002 V1 Exchange Server Security Certificate Information Leakage Vulnerability
6668	Microsoft Content Management Server Cross-Site Scripting Vulnerability
668	Microsoft MSN Setup BBS ActiveX Control Buffer Overflow Vulnerability
8221	Microsoft MSN Messenger Image File Transfer Denial of Service Vulnerability
8281	Microsoft Outlook Express Script Execution Weakness
8533	Microsoft Word Macro Execution Security Model Bypass Vulnerability
8761	Microsoft Word Malformed Document Denial of Service Vulnerability
9082	Microsoft MSN Messenger Information Leakage Weakness
9342	Microsoft Word Form Protection Password Removal Weakness
9673	Microsoft Outlook Express Arbitrary Program Execution Vulnerability
9709	Multiple Outlook/Outlook Express Predictable File Location Weaknesses

Bugtraq ID	Title
9798	Microsoft Internet Explorer window.open Search Pane Cross-Zone Scripting Vulnerability
9832	WU-FTPD restricted-gid Unauthorized Access Vulnerability
9835	IBM AIX Rexecd Privilege Escalation Vulnerability
9837	Sun Solaris Multiple Unspecified Local UUCP Buffer Overrun Vulnerabilities
9841	Multiple Vendor Internet Browser Cookie Path Argument Restriction Bypass Vulnerability
9852	Sun Solaris Patch Unexpected Security Weakness
9869	Opera Web Browser Large JavaScript Array Handling Vulnerability
9878	Windows Media Services MX_STATS_LogLine NSIISlog.DLL Remote Buffer Overflow Vulnerability
9892	Microsoft Windows XP explorer.exe Remote Denial of Service Vulnerability

March 9, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 26 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
9743	Microsoft ASN.1 Library Multiple Stack-Based Buffer Overflow Vulnerabilities
8262	Microsoft DirectShow MIDI Filetype Buffer Overflow Vulnerability
9761	Microsoft Internet Explorer Cross-Domain Event Leakage Vulnerability
5610	Microsoft Internet Explorer HTML Same Origin Policy Violation Vulnerability
5672	Microsoft Internet Explorer IFrame/Frame Cross-Site/Zone Script Execution Vulnerability
6217	Microsoft Internet Explorer Object Tag Temporary Internet File Folder Vulnerability

Bugtraq ID	Title
6216	Microsoft Internet Explorer PNG Buffer Overflow Vulnerability
2963	Microsoft Internet Explorer Unauthorized Document Object Model Access Vulnerability
9769	Microsoft Internet Explorer window.open Media Bar Cross-Zone Scripting Vulnerability
9828	Microsoft MSN Messenger Information Disclosure Vulnerability
9827	Microsoft Outlook Mailto Parameter Quoting Zone Bypass Vulnerability
9825	Microsoft Windows Media Services Remote Denial of Service Vulnerability
9707	Microsoft Windows XP explorer.exe Multiple Memory Corruption Vulnerabilities
9747	Mozilla Browser Zombie Document Cross-Site Scripting Vulnerability
1298	Multiple Vendor xterm (and derivatives) Denial of Service Vulnerability
9759	Sun Solaris conv_fix Unspecified File Overwrite Vulnerability
9757	Sun Solaris Unspecified Passwd Local Root Compromise Vulnerability
326	X11R6 3.3.3 Symlink Vulnerability
2985	XDM Session Cookie Guessing Vulnerability
3965	XFree86 4.1.0 Missing authDomain Unauthorized xdm Connection Vulnerability
3657	XFree86 fbglyph Denial of Service Vulnerability
9636	XFree86 Font Information File Buffer Overflow Vulnerability
8682	XFree86 XLOCALEDIR Buffer Overflow Variant Vulnerability
7002	XFree86 XLOCALEDIR Local Buffer Overflow Vulnerability
3030	XMan ManPath Environment Variable Buffer Overflow
3663	XTerm Title Bar Buffer Overflow Vulnerability

February 24, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 20 additional vulnerabilities. The following table includes information about the vulnerabilities

Bugtraq ID	Title
8231	CGI.pm Start_Form Cross-Site Scripting Vulnerability
9660	Microsoft IIS Unspecified Remote Denial Of Service Vulnerability
9663	Microsoft Internet Explorer Bitmap Processing Integer Overflow Vulnerability
9629	Microsoft Internet Explorer Double-Null URI Denial Of Service Vulnerability
9611	Microsoft Internet Explorer LoadPicture File Enumeration Weakness
9628	Microsoft Internet Explorer Shell: IFrame Cross-Zone Scripting Vulnerability
9643	Microsoft Internet Explorer Unauthorized Clipboard Contents Disclosure Vulnerability
9658	Microsoft Internet Explorer Unspecified CHM File Processing Arbitrary Code Execution Vulnerability
1282	Microsoft Media Service DoS Vulnerability
2123	Microsoft Windows Media Services Severed Connection DoS Vulnerability
1655	Microsoft Windows Media Unicast Services DoS Vulnerability
9621	Microsoft Windows XP HCP URI Handler Arbitrary Command Execution Vulnerability
9685	Microsoft Windows XP Help And Support Center Interface Spoofing Weakness
9640	Opera Web Browser CLSID File Extension Misrepresentation Vulnerability
6111	Safe.PM Unsafe Code Execution Vulnerability
9637	Samba Mksmbpasswd.sh Insecure User Account Creation Vulnerability
9477	Sun Solaris modload() Unauthorized Kernel Module Loading Vulnerability
9534	Sun Solaris PExec Custom Profile Arbitrary Privileges Vulnerability
9548	Sun Solaris TCSetAttr System Hang Denial Of Service Vulnerability

Bugtraq ID	Title
9145	Yahoo! Messenger YAuto.DLL Open Buffer Overflow Vulnerability

February 10, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports ten additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
9471	Apache mod_perl Module File Descriptor Leakage Vulnerability
7871	IBM AIX LSMCODE Environment Variable Local Buffer Overflow Vulnerability
9510	Microsoft Internet Explorer CLSID File Extension Misrepresentation Vulnerability
9568	Microsoft Internet Explorer NavigateAndFind() Cross-Zone Policy Vulnerability
9633	Microsoft ASN.1 Library Length Integer Mishandling Memory Corruption Vulnerability
9624	Microsoft Windows Internet Naming Service Buffer Overflow Vulnerability
9487	Microsoft Windows XP Explorer Self-Executing Folder Vulnerability
9635	Microsoft Windows ASN.1 Library Bit String Processing Integer Handling Vulnerability
3064	Multiple Vendor Telnetd Buffer Overflow Vulnerability
9507	TCPDump ISAKMP Decoding Routines Denial Of Service Vulnerability

February 3, 2004

This content update for Symantec Vulnerability Assessment 1.0 enhances detection of the following three vulnerabilities.

Bugtraq ID	Title
9108	Microsoft Internet Explorer Window.MoveBy/Method Caching Mouse Click Event Hijacking Vulnerability
9109	Microsoft Internet Explorer BackToFramedJPU Cross-Domain Policy Vulnerability
9182	Multiple Browser URI Display Obfuscation Weakness

January 27, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports twelve additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
9420	HP SharedX Unspecified Local Insecure File Access Vulnerability
7346	IBM FTP Daemon Kerberos 5 Unspecified Administrative Access Vulnerability
9114	ISC BIND Negative Cache Poison Denial Of Service Vulnerability
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
9118	Microsoft Exchange Server 2003 Outlook Web Access Lowered Security Settings Weakness
6241	Multiple Vendor X Font Server Remote Buffer Overrun Vulnerability
1870	tcpdump AFS ACL Packet Buffer Overflow Vulnerability
9423	TCPDump ISAKMP Decoding Routines Multiple Remote Buffer Overflow Vulnerabilities
9263	Tcpdump L2TP Parser Remote Denial of Service Vulnerability

Bugtraq ID	Title
313	Tcpdump Protocol Four and Zero Header Length Vulnerability

January 14, 2004

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 20 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
8207	Microsoft ISA Server Cross-Site Scripting Vulnerabilities
9409	Microsoft Exchange Server 2003 Outlook Web Access Random Mailbox Access Vulnerability
9278	Microsoft Internet Explorer File Download Warning Bypass Vulnerability
9295	Microsoft Internet Explorer HTTP Referer Information Disclosure Vulnerability
9335	Microsoft Internet Explorer Malicious Shortcut Self-Executing HTML Vulnerability
9320	Microsoft Internet Explorer showHelp CHM File Execution Weakness
8565	Microsoft Internet Explorer XML Page Object Type Validation Vulnerability
9408	Microsoft ISA Server 2000 H.323 Filter Remote Buffer Overflow Vulnerability
3198	Microsoft ISA Server Cross-Site Scripting Vulnerability
3501	Microsoft ISA Server Denial of Service Vulnerability
7145	Microsoft ISA Server DNS Intrusion Filter Denial of Service Vulnerability
7623	Microsoft ISA Server Error Page Cross-Site Scripting Vulnerability
3196	Microsoft ISA Server H.323 Memory Leak Denial of Service Vulnerability
3197	Microsoft ISA Server Proxy Service Memory Leak Denial of Service Vulnerability
2600	Microsoft ISA Server Web Proxy DoS Vulnerability
9407	Microsoft MDAC Function Broadcast Response Buffer Overrun Vulnerability

Bugtraq ID	Title
9281	Opera Browser URI Display Obfuscation Weakness
9280	Sun Solaris tcsh ls-F Builtin Unspecified Privilege Escalation Vulnerability
7064	Sun SUNWldap Library Hostname Buffer Overflow Vulnerability
9383	Yahoo! Messenger File Transfer Buffer Overrun Variant Vulnerability

December 30, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 23 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
7720	CDE DTSession Unspecified Privilege Escalation Vulnerability
7493	Ethereal Multiple Dissector One Byte Buffer Overflow Vulnerabilities
4630	CDE DTPrintInfo Help Volume Search Buffer Overflow Vulnerability
7719	CDE DTPrintInfo Unspecified Privilege Escalation Vulnerability
2603	CDE dtsession Buffer Overflow Vulnerability
7730	CDE LibDTHelp Unspecified Privilege Escalation Vulnerability
7732	CDE LibDTSvc Unspecified Privilege Escalation Vulnerability
6567	Ethereal LMP Dissector Malformed Packet Memory Corruption Vulnerability
5166	Ethereal LMP Dissector Memory Corruption Vulnerability
7881	Ethereal Multiple Dissector String Handling Vulnerabilities
7050	Ethereal NTLMSSP Dissector Heap Corruption Vulnerability
7495	Ethereal PPP Dissector Integer Overflow Vulnerability
4806	Ethereal Server Message Block Dissector Malformed Packet Denial Of Service Vulnerability
7879	Ethereal SPNEGO Dissector Denial Of Service Vulnerability
5582	HP-UX LPAdmin Unspecified Buffer Overflow Vulnerability
9255	IBM AIX diag Unspecified Privilege Escalation Vulnerability

Bugtraq ID	Title
9254	IBM AIX enq Local Format String Vulnerability
3400	RPCBind / Portmap Malformed RPC Request Denial of Service Vulnerability
5040	Solaris 8 dtscreen Authentication Bypass Vulnerability
4632	Solaris AdminTool Media Installation Path Buffer Overflow Vulnerability
1348	Solaris ufsrestore Buffer Overflow Vulnerability
9225	Sun Solaris LPStat Unspecified Local Privilege Escalation Vulnerability
9199	Sun Solaris Text Editor ed Temporary File Creation Vulnerability

December 17, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 41 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
9170	CDE DTPrintInfo Home Environment Variable Buffer Overflow Vulnerability
1972	Ethereal AFS Buffer Overflow Vulnerability
5167	Ethereal AFS Dissector Memory Corruption Vulnerability
4604	Ethereal ASN.1 String Memory Allocation Denial Of Service Vulnerability
6565	Ethereal BGP Dissector Infinite Loop Denial of Service Vulnerability
7878	Ethereal DCERPC Dissector Memory Allocation Vulnerability
4807	Ethereal DNS Dissector Infinite Loop Denial of Service Vulnerability
4808	Ethereal GIOP Dissector Memory Exhaustion Vulnerability
5573	Ethereal ISIS Dissector Memory Corruption Vulnerability
4168	Ethereal Malformed SNMP Denial of Service Vulnerability
7494	Ethereal Mount Dissector Integer Overflow Vulnerability
5165	Ethereal RSVP Dissector Memory Corruption Vulnerability
5163	Ethereal SOCKS Dissector Memory Corruption Vulnerability

Bugtraq ID	Title
7883	Ethereal TVB_GET_NSTRINGZ0) Memory Handling Vulnerability
3240	HP-UX Line Printer Daemon Buffer Overflow Vulnerability
9141	HP-UX Shar Utility Predictable Temporary File Creation Vulnerability
6800	HPUX Wall Message Buffer Overflow Vulnerability
5732	Joe Text Editor Backup SetUID Executable Editing Permission Elevation Vulnerability
1594	Microsoft FrontPage/IIS Cross Site Scripting shtml.dll Vulnerability
9216	Microsoft Internet Explorer Unspecified Remote Compromise Vulnerability
2988	Microsoft Windows 2000 SMTP Improper Authentication Vulnerability
4205	Microsoft Windows SMTP Service Authorization Bypass Vulnerability
5753	Mozilla Browser Large HTTP Header Buffer Overflow Vulnerability
5759	Mozilla document.open() Memory Corruption Denial of Service Vulnerability
5741	Mozilla Netscape Navigator Plug-In Path Disclosure Vulnerability
5694	Mozilla OnUnload Referer Information Leakage Vulnerability
3743	Mozilla Predictable Temporary File Symbolic Link Attack Vulnerability
5766	Mozilla XMLSerializer Same Origin Policy Violation Vulnerability
9182	Multiple Browser URI Display Obfuscation Weakness
8951	Multiple Ethereal Protocol Dissector Vulnerabilities
1165	Multiple Sniffer Vendor DNS Decode Vulnerability
9208	Multiple Vendor IKE Implementation Certificate Authenticity Verification Vulnerability
4098	Opera Content-Type HTML File Execution Vulnerability
9021	Opera Web Browser Opera. URI Handler Directory Traversal Vulnerability
4631	Solaris cachefs Buffer Overrun Vulnerability
4634	Solaris cachefs Denial of Service Vulnerability
2550	Solaris ftpd glob() Expansion LIST Heap Overflow Vulnerability
6709	Solaris in.ftpd Remote Denial of Service Vulnerability
3274	Solaris lpd Remote Command Execution Vulnerability

Bugtraq ID	Title
9147	Sun Solaris XSun Direct Graphics Access Insecure Temporary File Vulnerability
9158	Yahoo! Messenger IMVironment Cross-Site Scripting Vulnerability

December 3, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 34 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
9021	Opera Web Browser Opera. URI Handler Directory Traversal Vulnerability
6942	DTTerm Window Title Reporting Escape Sequence Command Execution Vulnerability
9062	HP-UX CDE dtmailpr Display Environment Variable Buffer Overrun Vulnerability
9063	HP-UX DCE Unspecified Remote Denial Of Service Vulnerability
9078	IBM AIX RCP Utility Local Buffer Overrun Vulnerability
9109	Microsoft Internet Explorer BackToFramedJPU Cross-Domain Policy Vulnerability
9107	Microsoft Internet Explorer Browser MHTML Redirection Local File Parsing Vulnerability
9106	Microsoft Internet Explorer Invalid ContentType Cache Directory Location Disclosure Weakness
9105	Microsoft Internet Explorer MHTML Forced File Execution Vulnerability
9108	Microsoft Internet Explorer Window.MoveBy/Method Caching Mouse Click Event Hijacking Vulnerability
8523	Multiple Vendor PC2Phone Software Remote Denial of Service Vulnerability
7430	Opera 7.10 Permanent Denial Of Service Vulnerability
4834	Opera Arbitrary File Disclosure Vulnerability
6962	Opera Automatic Redirection Cross Site Scripting Vulnerability

Bugtraq ID	Title
4098	Opera Content-Type HTML File Execution Vulnerability
5401	Opera FTP View Cross-Site Scripting Vulnerability
8853	Opera HREF Malformed Server Name Heap Corruption Vulnerability
7449	Opera JavaScript Console Single Quote Attribute Injection Vulnerability
7271	Opera JavaScript Java Method Access Vulnerability
7056	Opera Long Filename Download Buffer Overrun Vulnerability
7450	Opera Long Filename Remote Heap Corruption Vulnerability
9019	Opera Multiple MIME Type File Dropping Weakness
7294	Samba 'call_trans2open' Remote Buffer Overflow Vulnerability
7295	Samba Multiple Unspecified Remote Buffer Overflow Vulnerabilities
6210	Samba Server Encrypted Password Buffer Overrun Vulnerability
4173	Yahoo! Instant Messenger Plain Text Password Vulnerability
4838	Yahoo! Instant Messenger Script Injection Vulnerability
5579	Yahoo! Instant Messenger Signed Content Weakness
4164	Yahoo! Instant Messenger Spoofed Username Vulnerability
4837	Yahoo! Messenger Call Center Buffer Overflow Vulnerability
8894	Yahoo! Messenger File Transfer Buffer Overrun Vulnerability
4163	Yahoo! Messenger IMvironment Field Overflow Vulnerability
4162	Yahoo! Messenger Message Field Overflow Vulnerability

November 20, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 32 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
8926	Apache Web Server mod_cgid Module CGI Data Redirection Vulnerability

Bugtraq ID	Title
8911	Apache Web Server Multiple Module Local Buffer Overflow Vulnerability
1889	CDE DTterm Terminal Name Buffer Overflow Vulnerability
8875	Coreutils LS Width Argument Integer Overflow Vulnerability
8985	HP-UX NLSPATH Environment Variable Format String Vulnerability
3561	HP-UX Remote Line Printer Daemon Logic Flaw Vulnerability
3701	HP-UX RLPDaemon Arbitrary Log File Creation Vulnerability
6837	HP-UX rs.F3000 Unspecified Unauthorized Access Vulnerability
8986	HP-UX Software Distributor Lang Environment Variable Local Buffer Overrun Vulnerability
9009	Microsoft Internet Explorer DHTML Drag and Drop Local File Saving Vulnerability
8980	Microsoft Internet Explorer Double Slash Cache Zone Bypass Vulnerability
9015	Microsoft Internet Explorer ExecCommand Cross-Domain Access Violation Vulnerability
9022	Microsoft Internet Explorer file.writeline Local File Writing Vulnerability
9014	Microsoft Internet Explorer Function Pointer Override Cross-Domain Access Violation Vulnerability
9013	Microsoft Internet Explorer Script URL Cross-Domain Access Violation Vulnerability
8984	Microsoft Internet Explorer Self Executing HTML Arbitrary Code Execution Vulnerability
9012	Microsoft Internet Explorer XML Object Zone Restriction Bypass Vulnerability
9011	Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability
524	Multiple Vendor rpc.cmsd Buffer Overflow Vulnerability
9040	OpenSSH PAM Conversation Memory Scrubbing Weakness
5587	Samba Improperly Terminated Struct Buffer Overflow Vulnerability
2617	Samba Insecure TMP file Symbolic Link Vulnerability
7107	Samba REG File Writing Race Condition Vulnerability

Bugtraq ID	Title
2928	Samba Remote Arbitrary File Creation Vulnerability
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
4624	Solaris admintool Local Buffer Overflow Vulnerability
4633	Solaris LBXProxy Display Name Buffer Overflow Vulnerability
8929	Sun Solaris NFS Server Unspecified Remote Denial Of Service Vulnerability
8893	Wu-Ftpd S/Key Remote Buffer Overrun Vulnerability

Content updates for Symantec Vulnerability Assessment 1.0 can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

November 11, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports one additional vulnerability. The following table includes information about the vulnerability.

Bugtraq ID	Title
9011	Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability

November 6, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 44 additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
8795	CDE DTPrintInfo Display Environment Variable Buffer Overflow Vulnerability

Bugtraq ID	Title
5162	Ethereal BGP Dissector Buffer Overflow Vulnerability
7880	Ethereal OSI Dissector Buffer Overflow Vulnerability
6563	Ethereal PPP Dissector Malformed Packet Memory Corruption Vulnerability
7049	Ethereal SOCKS Dissector Format String Vulnerability
6564	Ethereal TDS Dissector Malformed Packet Memory Corruption Vulnerability
5164	Ethereal WCP Dissector Buffer Overflow Vulnerability
4805	Ethereal X11 Dissector Buffer Overflow Vulnerability
3728	Exim Pipe Hostname Arbitrary Command Execution Vulnerability
8418	HP Fixes Unspecified Local Denial Of Service Vulnerability
8311	HP-UX Unspecified Network Traffic Program Failure Denial Of Service Vulnerability
3950	Linux ICMP Kernel Information Leakage Vulnerability
4699	Linux NetFilter NAT Information Leakage Vulnerability
8830	Microsoft ActiveX Authenticode Verification Bypass Vulnerability
8832	Microsoft Exchange Server 5.5 Outlook Web Access Cross-Site Scripting Vulnerability
8454	Microsoft Internet Explorer BR549.DLL ActiveX Control Buffer Overflow Vulnerability
8556	Microsoft Internet Explorer Browser Popup Window ObjectType Validation Vulnerability
8456	Microsoft Internet Explorer Browser Popup Window ObjectType Validation Vulnerability
8886	Microsoft Internet Explorer Local Resource Reference Vulnerability
8874	Microsoft Internet Explorer Scrollbar-Base-Color Partial Denial Of Service Vulnerability
8565	Microsoft Internet Explorer XML Page Object Type Validation Vulnerability
8457	Microsoft Internet Explorer Zone Restriction Bypass Script Execution Vulnerability
8827	Microsoft ListBox/ComboBox Control User32.dll Function Buffer Overrun Vulnerability

Bugtraq ID	Title
8833	Microsoft Windows 2000 TroubleShooter ActiveX Control Buffer Overflow Vulnerability
8828	Microsoft Windows Help And Support Center URI Handler Buffer Overflow Vulnerability
5757	Mozilla Browser HTTP/HTTPS Redirection Weakness
5403	Mozilla FTP View Cross-Site Scripting Vulnerability
5739	Mozilla Multiple Vulnerabilities
5762	Mozilla Space Key XPI Installation Vulnerability
5742	Netscape/Mozilla Javascript Array Object Heap Corruption Vulnerability
8628	OpenSSH Buffer Mismanagement Vulnerabilities
8641	Sendmail Prescan() Variant Remote Buffer Overrun Vulnerability
7240	Solaris dtsession HOME Buffer Overflow Vulnerability
6080	Sun Solaris 8 KMEM_FLAGS Kernel Parameter Denial Of Service Vulnerability
8253	Sun Solaris automountd Denial of Service Vulnerability
8079	Sun Solaris Full UFS File System Kernel Panic Denial Of Service Vulnerability
6318	Sun Solaris Libthread Library Denial of Service Vulnerability
8836	Sun Solaris Pipe Function Unspecified Kernel Race Condition Vulnerability
7455	Sun Solaris RPCbind Unspecified Denial of Service Vulnerability
8831	Sun Solaris SysInfo System Call Kernel Memory Reading Vulnerability
7820	Sun Solaris Syslogd UDP Packet Buffer Overflow Denial Of Service Vulnerability
7794	Sun Solaris Telnet Daemon Remote Denial Of Service Vulnerability
7835	Sun Solaris UTMP_Update Buffer Overflow Vulnerability
6509	Sun Solaris Wall Spoofed Message Origin Vulnerability

October 23, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 52 vulnerabilities for host machines. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
N/A	AIX Buffer Overflow in DNS resolver Read Code
N/A	AIX Buffer Overflow in nslookup
N/A	AIX Buffer Overflow in some NIS Commands
N/A	AIX Diag Script could Allow Root Access
N/A	AIX DNS resolver buffer overflow
N/A	AIX ftpd Buffer Overflow Vulnerability
N/A	AIX insecure temporary files in dhcp scripts
N/A	AIX libnsl Integer Overflow Vulnerability
N/A	AIX login may core dump with too many environment variables after user name
N/A	AIX lsattr Core Dumps with Long Argument
N/A	AIX lsmcode command line usage
N/A	AIX lsmcode may crash with invalid argument
N/A	AIX Mailx and Mail Core Dump With Long Argument
N/A	AIX namerslv Core Dumps with Long Argument
N/A	AIX nice and nohup Core Dump when Passed Extremely Long Arguments
N/A	AIX permissions in /usr/filesystem should not be writable
N/A	AIX resolver DoS and named Code Execution
N/A	AIX rpc Service DoS
N/A	AIX sendmail Mime Header Length
N/A	AIX Some TCP/IP Commands Core Dump With Long Arguments
N/A	AIX Traceroute may Core Dump with Long Parameter
N/A	AIX uucp segmentation fault with long arguments
N/A	AIX various perfstat flags don't require root privileges

Bugtraq ID	Title
N/A	AIX xfs Remote Buffer Overflow Vulnerability
N/A	AIX ypserv
8707	Apache htpasswd Password Entropy Weakness
3487	CDE DTPrintInfo Session Option Buffer Overflow Vulnerability
8803	IBM "cu" Unspecified Buffer Overflow Vulnerability
8805	IBM AIX Bellmail Race Condition Vulnerability
8738	IBM AIX GetIPNodeByName API Socket Management Vulnerability
3070	IBM AIX LANG Environment Variable Buffer Overflow Vulnerability
8806	IBM AIX libdiag Trace File Symlink Vulnerability
8448	IBM AIX tsm Utility Local Format String Vulnerability
8801	IBM AIX UUQ Buffer Overflow Vulnerability
8802	IBM dump_smutil.sh Insecure Temporary File Creation Vulnerability
8812	IBM OpenGL XGLInfo Program Screen Option Negative Value Abnormal End
8808	IBM policyd and rsvpd Insecure Temporary File Creation Vulnerability
8807	IBM VMM Performance Tools Insufficient Access Controls Privilege Elevation
8758	Microsoft Internet Explorer Absolute Position Block Denial Of Service
7640	Microsoft Windows Media Player Automatic File Download and Execution
8783	Microsoft Windows Message Queuing Service Heap Overflow Vulnerability
8747	Microsoft Windows PostThreadMessage() Arbitrary Process Killing Vulnerability
8811	Microsoft Windows RPCSS Multi-thread Race Condition Vulnerability
3382	Multiple CDE Vendor ToolTalk Database Server Format String Vulnerability
8804	Multiple IBM AIX MUXATMD Buffer Overrun Vulnerabilities
5082	Multiple Vendor CDE ToolTalk Database Server Null Write Vulnerability
5083	Multiple Vendor CDE ToolTalk Database Server Symbolic Link Vulnerability
6001	Multiple Vendor IPSec Implementation Denial of Service Vulnerabilities
3681	Multiple Vendor System V Derived 'login' Buffer Overflow Vulnerability

Bugtraq ID	Title
8674	Sendmail Headers Prescan Denial Of Service Vulnerability
8727	Sun Solaris Serial Console Excessive Output Data Denial of Service Vulnerability
8668	Wu-Ftpd SockPrintf() Remote Stack-based Buffer Overrun Vulnerability

Content updates for Symantec Vulnerability Assessment 1.0 can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

If Windows SESA agents return an unknown state for Internet Explorer safeguards, restart their SESA agent services.

October 15, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports two critical Microsoft vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
8826	Microsoft Messenger Service Buffer Overrun Vulnerability
8838	Microsoft Exchange Server Buffer Overflow Vulnerability

Content updates for Symantec Vulnerability Assessment 1.0 can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

October 8, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports two additional vulnerabilities. The following table includes information about the vulnerabilities.

Bugtraq ID	Title
7264	IBM AIX secldapclntd Unauthorized Data Access Vulnerability
5885	IBM AIX ERRPT Local Buffer Overflow Vulnerability

Content updates for Symantec Vulnerability Assessment 1.0 can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

Resolved issues: False positives have been reported in some environments for Bugtraq IDs 5872, 7727, 1514, 1507, 2303, and 2348. These issues are now resolved.

September 24, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports ten additional vulnerabilities. It can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

The following table includes information about the vulnerabilities:

Bugtraq ID	Title
8646	IBM AIX lpd Local Format String Vulnerability
8555	Microsoft Exchange Server SMTP HELO Argument Buffer Overflow Vulnerability
8556	Microsoft Internet Explorer Browser Popup Window Object Type Validation Vulnerability
8565	Microsoft Internet Explorer XML Page Object Type Validation Vulnerability
8530	Microsoft mshtml.dll Library GIF Image Handling Denial of Service Vulnerability
8532	Microsoft Windows NetBIOS Name Service Reply Information Leakage Weakness
8531	Microsoft Windows XP TCP Packet Information Leakage Vulnerability
8577	Multiple Microsoft Internet Explorer Script Execution Vulnerabilities
8615	Sun Solaris SAdmin Client Credentials Remote Administrative Access Vulnerability
1924	Windows NT 4.0 Terminal Server RegAPI.DLL Buffer Overflow

September 16, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports one new vulnerability. It can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

The following table includes information about the vulnerability.

Bugtraq ID	Title
8615	Sun Solaris SAdmin Client Credentials Remote Administrative Access Vulnerability

September 11, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports eight additional vulnerabilities. It can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

The following table includes information about the vulnerabilities:

Bugtraq ID	Title
8454	Microsoft Internet Explorer BR549.DLL ActiveX Control Buffer Overflow Vulnerability
8456	Microsoft Internet Explorer Object Type Validation Vulnerability
8457	Microsoft Internet Explorer Zone Restriction Bypass Script Execution Vulnerability
8458	Microsoft RPCSS DCERPC DCOM Object Activation Packet Length Heap Corruption Vulnerability
8459	Microsoft RPCSS DCOM Interface Long Filename Heap Corruption Vulnerability
5535	Microsoft Terminal Services Inactive Console Screensaver Lock Failure Weakness
8098	Microsoft Windows 2000 Terminal Services Named Pipe System Account Access Vulnerability
5376	Microsoft Windows Terminal Services Denial Of Service Vulnerability

August 28, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports five additional vulnerabilities. It can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

The following table includes information about the vulnerabilities:

Bugtraq ID	Title
6065	Apache 2 WebDAV CGI POST Request Information Disclosure Vulnerability
7930	Microsoft Windows 2000 Active Directory Remote Stack Overflow Vulnerability
8045	Microsoft Windows 2000 SP4 Released - Multiple Vulnerabilities Fixed
8314	Sun Solaris PSIG Kernel Panic Denial Of Service Vulnerability
4639	Sun Solaris RWall Daemon Syslog Format String Vulnerability

August 12, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 31

vulnerabilities. It can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

The following table includes information about the vulnerabilities:

Bugtraq ID	Title
8226	Apache HTTP Server Multiple Vulnerabilities
7768	Apache Tomcat Insecure Directory Permissions Vulnerability
8137	Apache Web Server Prefork MPM Denial Of Service Vulnerability
8134	Apache Web Server SSLCipherSuite Weak CipherSuite Renegotiation Weakness
8138	Apache Web Server Type-Map Recursive Loop Denial Of Service Vulnerability
8169	Microsoft Internet Explorer AutoScan Method Browser Security Policy Violation Weakness
8176	Microsoft Internet Explorer window.createPopup Interface Spoofing Vulnerability
8113	Microsoft Outlook Web Access HTML Attachment Script Execution Vulnerability
8114	Microsoft RundLL32.EXE Buffer Overflow Vulnerability
8195	Microsoft SMTP Service Invalid FILETIME Denial of Service Vulnerability
8261	Microsoft SQL Server / MSDE Multiple Vulnerabilities
8274	Microsoft SQL Server / MSDE Named Pipe Denial Of Service Vulnerability
8276	Microsoft SQL Server / MSDE Named Pipes Privilege Escalation Vulnerability
8275	Microsoft SQL Server LPC Port Request Buffer Overflow Vulnerability
8083	Microsoft Windows 2000 Domain Controller Spoofing Vulnerability
8086	Microsoft Windows 2000 Port Name Buffers Potential Buffer Overflow Vulnerability
8234	Microsoft Windows 2000 RPC DCOM Interface Denial of Service Vulnerability

Bugtraq ID	Title
8090	Microsoft Windows 2000 ShellExecute() Buffer Overflow Vulnerability
8089	Microsoft Windows 2000 Unspecified Cryptnet.DLL Memory Leakage Vulnerability
8081	Microsoft Windows 2000 USBH_IocctlGetNodeConnectionDriver
8154	Microsoft Windows Accessibility Utility Manager Privilege Escalation Vulnerability
8084	Microsoft Windows IMAADPCM cbDestLength Buffer Overrun Vulnerability
8263	Microsoft Windows Media Player IE Zone Access Control Bypass Vulnerability
8259	Microsoft Windows NT File Management Function Denial Of Service Vulnerability
8087	Microsoft Windows Security Accounts Manager API Denial Of Service Vulnerability
8208	Microsoft Windows XP Shell Desktop.ini Buffer Overflow Vulnerability
7148	OpenSSL Bad Version Oracle Side Channel Attack Vulnerability
7101	OpenSSL Timing Attack RSA Private Key Information Disclosure Vulnerability
8094	SSH Communications Secure Shell/IPSEC Express Toolkit RSA Signature Forging Vulnerability
8054	Sun Solaris Deadlock Kernel Panic Vulnerability
8250	Sun Solaris IPv6 Packet Denial of Service Vulnerability

July 29, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports eight additional vulnerabilities for Microsoft Windows. It can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

The following table includes information about the vulnerabilities:

Bugtraq ID	Title
8092	Microsoft IIS_VTI_BOT Malicious WebBot Elevated Permissions Vulnerability
8152	Microsoft SMB Request Handler Buffer Overflow Vulnerability
8093	Microsoft Windows 2000 Active Directory Forest Origin Validation Vulnerability
7930	Microsoft Windows 2000 Active Directory Remote Stack Overflow Vulnerability
8085	Microsoft Windows 2000 ModifyDN Request Denial of Service Vulnerability
8128	Microsoft Windows CreateFile API Named Pipe Privilege Escalation Vulnerability
8016	Microsoft Windows HTML Converter HR Align Buffer Overflow Vulnerability
8035	Microsoft Windows Media Services NSIISlog.DLL Remote Buffer Overflow Vulnerability

July 17, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports one new vulnerability. It can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

The following table includes information about the vulnerability.

Bugtraq ID	Title
8205	Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability

July 15, 2003

This content update for Symantec Vulnerability Assessment 1.0 detects and reports 81 additional vulnerabilities. It can be downloaded only using the LiveUpdate feature of Symantec Vulnerability Assessment.

The following table includes information about the vulnerabilities:

Bugtraq ID	Title
7725	Apache Basic Authentication Module Valid User Login Denial Of Service Vulnerability
7827	HP-UX Unspecified Network Traffic Denial Of Service Vulnerability
7798	HP-UX UUSUB System Hostname Buffer Overflow Vulnerability
7604	IBM AIX Multiple Unspecified Security Vulnerabilities
4583	Internet Explorer Recursive JavaScript Event Denial of Service Vulnerability
606	Microsoft HTML Form Control DoS Vulnerability
2463	Microsoft IE Telnet Client File Overwrite Vulnerability
861	Microsoft IE5 vnd.ms.radio URL Vulnerability
7733	Microsoft IIS ASP Header Denial Of Service Vulnerability
7731	Microsoft IIS Redirection Error Page Cross-Site Scripting Vulnerability
7734	Microsoft IIS SSINC.DLL Server Side Includes Buffer Overflow Vulnerability
3339	Microsoft Index Server 2.0 File Information and Path Disclosure Vulnerability
2709	Microsoft Index Server Buffer Overflow Vulnerability
2269	Microsoft Index Server Webhits.dll ASP Source Disclosure Vulnerability
1861	Microsoft Indexing Services .htw Cross-Site Scripting Vulnerability
7826	Microsoft Internet Explorer %USERPROFILE% File Execution Weakness
7057	Microsoft Internet Explorer .MHT File Buffer Overflow Vulnerability
2081	Microsoft Internet Explorer 3.01 Remote .lnk/.url Vulnerability
1978	Microsoft Internet Explorer 5.5 Index.dat Vulnerability
2046	Microsoft Internet Explorer 5.5 Print Template ActiveX Vulnerability

Bugtraq ID	Title
3670	Microsoft Internet Explorer About: URL Zone Spoofing Vulnerability
1394	Microsoft Internet Explorer and Outlook/Outlook Express Remote File Write Vulnerability
3116	Microsoft Internet Explorer Arbitrary HTML File Execution Vulnerability
4411	Microsoft Internet Explorer Cascading Style Sheet File Disclosure Vulnerability
7810	Microsoft Internet Explorer Classic Mode FTP Client Cross Domain Scripting Vulnerability
5094	Microsoft Internet Explorer CLASSID Denial of Service Vulnerability
7384	Microsoft Internet Explorer CLASSID Variant Denial Of Service Vulnerability
4085	Microsoft Internet Explorer Content-Type Field Arbitrary File Execution Vulnerability
4754	Microsoft Internet Explorer Cookie Content Disclosure Vulnerability
5027	Microsoft Internet Explorer CSSText Bold Font Denial Of Service Vulnerability
7939	Microsoft Internet Explorer Custom HTTP Error HTML Injection Vulnerability
7502	Microsoft Internet Explorer DHTML AnchorClick Partial Denial Of Service Vulnerability
6779	Microsoft Internet Explorer Dialog Box Cross-Domain Violation Vulnerability
3768	Microsoft Internet Explorer Directory Disclosure Vulnerability
6017	Microsoft Internet Explorer Document.Write() Zone Bypass Vulnerability
4371	Microsoft Internet Explorer DYNSRC File Information Disclosure Vulnerability
7763	Microsoft Internet Explorer False URL Information Vulnerability
5450	Microsoft Internet Explorer File Attachment Script Execution Vulnerability
2836	Microsoft Internet Explorer File Contents Disclosure Vulnerability
2833	Microsoft Internet Explorer File Disclosure Vulnerability
3892	Microsoft Internet Explorer Form Denial of Service Vulnerability

Bugtraq ID	Title
3767	Microsoft Internet Explorer GetObject File Disclosure Vulnerability
4505	Microsoft Internet Explorer History List Script Injection Vulnerability
2045	Microsoft Internet Explorer 'INPUT TYPE=FILE' Vulnerability
3469	Microsoft Internet Explorer JavaScript Desktop Spoofing Vulnerability
4392	Microsoft Internet Explorer Known Local File Script Execution Vulnerability
7706	Microsoft Internet Explorer Malformed JavaScript Denial of Service Vulnerability
4087	Microsoft Internet Explorer MIME Type File Extension Spoofing Vulnerability
3789	Microsoft Internet Explorer Modeless Dialog DoS Vulnerability
2129	Microsoft Internet Explorer 'mstask.exe' CPU Consumption Vulnerability
7938	Microsoft Internet Explorer MSXML XML File Parsing Cross-Site Scripting Vulnerability
1636	Microsoft Internet Explorer Navigate Function Cross Frame Access Vulnerability
3563	Microsoft Internet Explorer Password Character Determination Vulnerability
7491	Microsoft Internet Explorer Plugin.OCX EnableFullPage Input Validation Vulnerability
7420	Microsoft Internet Explorer Plugin.OCX Load() Method Buffer Overflow Vulnerability
6366	Microsoft Internet Explorer PNG Deflate Heap Corruption Vulnerability
3730	Microsoft Internet Explorer Refresh Denial of Service Vulnerability
3693	Microsoft Internet Explorer Remote File Viewing Vulnerability
1564	Microsoft Internet Explorer Scriptlet Rendering Vulnerability
6961	Microsoft Internet Explorer Self Executing HTML File Vulnerability
6780	Microsoft Internet Explorer ShowHelp Arbitrary Command Execution Vulnerability
5778	Microsoft Internet Explorer SSL Certificate Expiration Vulnerability

Bugtraq ID	Title
4519	Microsoft Internet Explorer Unicode Character Handling DoS Vulnerability
5730	Microsoft Internet Explorer URI Handler Restriction Circumvention Vulnerability
5490	Microsoft Internet Explorer XML Datasource Applet File Disclosure Vulnerability
3420	Microsoft Internet Explorer Zone Spoofing Vulnerability
4653	Microsoft Internet Explorer/Outlook Express XBM Handling DoS Vulnerability
7728	Microsoft Internet Information Service Multiple Vulnerabilities
4463	Microsoft VBScript ActiveX Word Object Denial Of Service Vulnerability
4158	Microsoft VBScript Same Origin Policy Violation Vulnerability
7788	Microsoft Windows 2000/XP/2003 IPV6 ICMP Flood Denial Of Service Vulnerability
7727	Microsoft Windows Media Services Logging ISAPI Buffer Overflow Vulnerability
7789	Microsoft Windows XP Nested Directory Denial of Service Vulnerability
5346	Multiple Browser Vendor Same Origin Policy Design Error Vulnerability
6028	Multiple Microsoft Internet Explorer Cached Objects Zone Bypass Vulnerability
3684	Multiple Vendor Image Count Denial of Service Vulnerability
3122	Multiple Vendor IMG Tag DoS Vulnerability
4322	Multiple Vendor JavaScript Interpreter Denial Of Service Vulnerability
7831	OpenSSH Reverse DNS Lookup Access Control Bypass Vulnerability
5366	OpenSSL ASN.1 Parsing Error Denial Of Service Vulnerability
7614	Sendmail Insecure Temporary File Privilege Escalation Vulnerability

