



VULNERABILITIES BULLETIN



KEY BENEFITS

Unmatched Security Intelligence

VeriSign® iDefense Security Intelligence Services leverage submissions from a private, worldwide network of independent security researchers obtained through our Vulnerability Contributor Program (VCP). Intelligence researchers are in over 30 countries and provide intelligence in 12 languages. VeriSign has received 1,100 submissions to the VCP in the last three years. Upon receipt of these submissions, VeriSign does thorough internal research to validate the submission, and upon validation, notifies both the affected vendor and VeriSign iDefense customers. VeriSign works closely with leading vendors to help ensure that any potential vulnerabilities are identified and that such vendors are able to create patches as quickly as possible, to the extent that such vendors determine that patches are necessary. Customers are also notified of these vulnerabilities, while VeriSign is working with the vendor. As a result, from the 1,100 VCP submissions over the past three years, VeriSign has reported more than 200 iDefense unique, original vulnerability reports to customers. Most important, VeriSign customers received notices regarding these vulnerabilities in advance of public disclosure by the vendors.

Proactive vulnerability notification is critical to effective risk management. VeriSign® iDefense Security Intelligence Services delivers comprehensive, actionable intelligence aiding customers in making decisions in response to threats on a real-time basis. The following is a list of VeriSign iDefense Exclusive Vulnerabilities that have been publicly disclosed by the vendor since January 1, 2005. The table shows the number of days VeriSign iDefense customers receive notification on exclusive vulnerabilities in advance of public disclosure.

IR#	TITLE	CLIENT DISCLOSURE	PUBLIC DISCLOSURE	LEAD TIME
413487	Multiple Vendor CHM lib Stack Overflow Vulnerability	7/7/05	10/28/05	113 days
414524	SCO Openserver backupsh Buffer Overflow Vulnerability	6/20/05	10/24/05	126 days
414525	SCO Openserver authsh Buffer Overflow Vulnerability	6/20/05	10/24/05	126 days
418472	SCO Unixware ppp prompt Buffer Overflow Vulnerability	8/23/05	10/24/05	62 days
411577	Symantec Norton AntiVirus 9.0 LiveUpdate Local Privilege Escalation Vulnerability	6/14/05	10/20/05	128 days
411657	Symantec Norton AntiVirus 9.0 DiskMountNotify Local Privilege Escalation Vulnerability	6/14/05	10/20/05	128 days
418937	Multiple Vendor ethereal srvloc Buffer Overflow Vulnerability	8/31/05	10/20/05	50 days
419655	Multiple Vendor wget/curl NTLM Buffer Overflow Vulnerability	9/7/05	10/13/05	36 days
415053	XMail sendmail Buffer Overflow Vulnerability	8/1/05	10/13/05	73 days
407911	Microsoft Distributed Transaction Controller TIP Denial of Service	3/21/05	10/11/05	204 days
407912	Microsoft Distributed Transaction Controller Packet Relay DoS Vulnerability	3/22/05	10/11/05	203 days
412188	Kaspersky Anti-Virus Engine CHM File Parser Buffer Overflow Vulnerability	6/7/05	10/10/05	125 days



Where it all comes together.™



VULNERABILITIES BULLETIN

Customized Intelligence

VeriSign® iDefense Security Intelligence Services offers a highly-customizable set of intelligence services delivering the intelligence your organization needs, when you need it.

The Value of Intelligence

The cost of a security breach in terms of loss of time, data, and brand equity has grown dramatically over the last few years. At the same time, the number of vulnerabilities has grown exponentially, while the time elapsed between vulnerability and exploit continues to shrink. As a result, it is increasingly critical for enterprises to proactively protect themselves. VeriSign, which tracks security events on a global basis, delivers notification of vulnerabilities and exploits as they are identified, providing timely, actionable information and guidance to help mitigate risks from such vulnerabilities or exploits. VeriSign® iDefense Security Intelligence Services enable a proactive approach to maintaining a secure environment, while saving time and money by eliminating the hours spent searching through Web sites and emails, gathering and distributing information, and following up on the results.

Security Monitoring and Risk Management

24/7 monitoring of security events, which are captured, analyzed and correlated in real-time by our Vulnerability Aggregation Team who provide primary and secondary analyses of new vulnerability exploits. Suspicious and malicious events are therefore proactively identified—helping to mitigate an organization’s risk potential.

IR#	TITLE	CLIENT DISCLOSURE	PUBLIC DISCLOSURE	LEAD TIME
413788	SGI Irix runpriv Local Privilege Escalation Vulnerability	7/26/05	10/10/05	76 days
415141	Linksys WRT54G Invalid Content-Length Denial of Service Vulnerability	7/6/05	10/5/05	91 days
410413	UW-IMAP Netmailbox Name Parsing Buffer Overflow Vulnerability	5/25/05	10/4/05	132 days
419199	Symantec AntiVirus Scan Engine Web Service Buffer Overflow Vulnerability	8/30/05	10/4/05	35 days
418055	RealNetworks RealPlayer/HelixPlayer RealPix Format String Vulnerability	8/3/05	9/30/05	58 days
418807	Clam AntiVirus Win32-UPX Buffer Overflow Vulnerability	8/22/05	9/19/05	28 days
418806	Clam AV Win32-FSG File Handling DoS Vulnerability	8/22/05	9/19/05	28 days
415138	Linksys WRT54G 'upgrade.cgi' Unauthenticated Firmware Upload Design Error Vulnerability	7/5/05	9/13/05	70 days
415136	Linksys WRT54G 'restore.cgi' Unauthenticated Configuration Modification Design Error Vulnerability	7/5/05	9/13/05	70 days
412945	Linksys WRT54G apply.cgi POST Buffer Overflow Vulnerability	5/24/05	9/13/05	112 days
411723	Linksys WRT54G Remote Administration Fixed Encryption Key Vulnerability	5/24/05	9/13/05	112 days
415462	GNU Mailutils 0.6 imap4d 'search' Format String Vulnerability	7/28/05	9/9/05	43 days
410918	3Com Network Supervisor Directory Traversal Vulnerability	5/20/05	9/1/05	104 days
410393	Novell NetMail IMAPD Command Continuation Request Heap Overflow	4/19/05	9/1/05	135 days
411690	Symantec AntiVirus Corporate Edition Local Privilege Escalation Vulnerability	6/14/05	8/29/05	76 days
414736	Adobe Version Cue VCNative Arbitrary File Overwrite Vulnerability	6/29/05	8/29/05	61 days
414734	Adobe Version Cue VCNative Arbitrary Library Loading Vulnerability	6/29/05	8/29/05	61 days
410415	AWStats ShowInfoURL Remote Command Execution Vulnerability	4/27/05	8/9/05	104 days
412440	Multiple Vendor Ethereal AFP Dissector Format String Vulnerability	6/16/05	8/5/05	50 days
415575	EMC Navisphere Manager Information Leakage Vulnerabilities	7/13/05	8/5/05	23 days



VULNERABILITIES BULLETIN

Global Network of Intelligence Contributors

VeriSign's multilingual network includes more than 200 research contributors in over 30 countries offering early and unique insight into the cyber underground and previously unknown software vulnerabilities.

IR#	TITLE	CLIENT DISCLOSURE	PUBLIC DISCLOSURE	LEAD TIME
408475	CA BrightStor ARCserve Backup Agent for SQL Buffer Overflow Vulnerability	4/14/05	8/2/05	110 days
413486	Clam AntiVirus .CHM File Handling Integer Overflow Vulnerability	7/6/05	7/25/05	19 days
409800	Sophos Anti-Virus Zip File Handling DoS Vulnerability	5/12/05	7/14/05	63 days
406955	Microsoft Word 2000 and 2002 Stack-Based Buffer Overflow Vulnerability	3/23/05	7/12/05	111 days
407117	Adobe Acrobat Reader for Linux Filespec Buffer Overflow Vulnerability	5/2/05	7/5/05	64 days
410407	Clam AntiVirus ClamAV Cabinet File Handling Denial of Service Vulnerability	5/18/05	6/29/05	42 days
411585	Clam AntiVirus MS-Expand File Handling Denial of Service Vulnerability	5/18/05	6/29/05	42 days
410457	Cacti config_settings.php Remote Code Execution Vulnerability	5/4/05	6/23/05	50 days
408167	Cacti top_graph_header.php Remote Code Execution Vulnerability	5/4/05	6/23/05	50 days
408167	Multiple Vendor Cacti Remote File Inclusion Vulnerability	5/4/05	6/23/05	50 days
408306	Veritas Backup Exec Agent CONNECT_CLIENT_AUTH Remote Buffer Overflow Vulnerability	3/16/05	6/23/05	99 days
408348	Veritas Backup Exec Agent Error Status Remote Denial of Service Vulnerability	3/16/05	6/23/05	99 days
407011	Veritas Backup Exec Server Remote Registry Access Vulnerability	3/16/05	6/23/05	99 days
412234	Veritas Backup Exec Remote Agent NDMLSRVR.DLL DoS Vulnerability	5/16/05	6/23/05	38 days
410083	RealNetworks RealPlayer RealText Parsing Heap Overflow Vulnerability	4/25/05	6/23/05	59 days
408198	IpSwitch WhatsUp Professional 2005 (SP1) SQL Injection Vulnerability	4/19/05	6/22/05	64 days
406405	Multiple Vendor Telnet Client Information Disclosure Vulnerability	2/14/05	6/14/05	120 days
410084	Microsoft Outlook Web Access Cross-Site Scripting Vulnerability	4/26/05	6/14/05	49 days
407338	Microsoft Interactive Training Buffer Overflow Vulnerability	2/23/05	6/14/05	110 days
409248	GNU Mailutils 0.6 mail header_get_field_name() Buffer Overflow Vulnerability	5/9/05	5/27/05	18 days
409241	GNU Mailutils imap4d Remote Format String Vulnerability	5/9/05	5/25/05	16 days



VULNERABILITIES BULLETIN

IR#	TITLE	CLIENT DISCLOSURE	PUBLIC DISCLOSURE	LEAD TIME
409244	GNU Mailutils imap4d FETCH Denial of Service Vulnerability	5/9/05	5/25/05	16 days
409246	GNU Mailutils 0.6 imap4d fetch_io Heap overflow Vulnerability	5/9/05	5/25/05	16 days
408853	Ipswitch iMAIL Remote LOGIN Denial of Service Vulnerability	4/20/05	5/25/05	35 days
408853	Ipswitch iMAIL Remote LOGIN Stack Overflow Vulnerability	4/20/05	5/25/05	35 days
408161	Ipswitch IMail IMAPD LSUB Denial of Service Vulnerability	4/20/05	5/24/05	34 days
408039	Ipswitch IMail Web Calendaring Arbitrary File Read Vulnerability	4/19/05	5/24/05	35 days
410454	Ipswitch IMail IMAP SELECT Command DoS Vulnerability	4/20/05	5/24/05	34 days
410697	Ipswitch IMail IMAPD STATUS Buffer Overflow Vulnerability	4/20/05	5/24/05	34 days
407614	Apple Mac OS X vpnd Server_id Buffer Overflow Vulnerability	3/30/05	5/4/05	34 days
406285	Apple Mac OS X NeST Buffer Overflow Vulnerability	2/16/05	5/3/05	75 days
406620	MySQL MaxDB Webtool Remote If Stack Overflow Vulnerability	4/11/05	4/26/05	15 days
406618	MySQL MaxDB Webtool Remote Stack Overflow Vulnerability	3/2/05	4/25/05	54 days
406617	MySQL MaxDB Webtool Remote Lock-Token Stack Overflow Vulnerability	2/28/05	4/25/05	56 days
406618	MySQL MaxDB Webtool Remote Denial of Service Vulnerability	3/2/05	4/25/05	53 days
408136	Microsoft Windows Explorer Document Metadata Embedded Command Vulnerability	3/7/05	4/19/05	42 days
404694	Mcafee Internet Security Suite 2005 Insecure ACL Vulnerability	2/1/05	4/18/05	76 days
405637	Microsoft Windows CSRSS.EXE Stack Overflow Vulnerability	1/3/05	4/12/05	98 days
408045	Microsoft Multiple E-Mail Client Address Spoofing Vulnerability	3/2/05	4/8/05	37 days
404357	SGI IRIX gr_osview Information Disclosure Vulnerability	2/8/05	4/7/05	58 days
404358	SGI IRIX gr_osview File Overwrite Vulnerability	2/8/05	4/7/05	57 days
404796	IBM Lotus Domino Server 6 Web Service Denial of Service Vulnerability	1/26/05	4/6/05	69 days
406541	PHP getimagesize() Denial of Service Vulnerability	2/22/05	3/31/05	37 days



VULNERABILITIES BULLETIN

IR#	TITLE	CLIENT DISCLOSURE	PUBLIC DISCLOSURE	LEAD TIME
406408	Multiple Telnet Client slc_add_reply() Buffer Overflow Vulnerability	2/14/05	3/28/05	42 days
404459	Mac OS X CF_CHARSET_PATH Buffer Overflow Vulnerability	2/1/05	3/21/05	48 days
407048	Computer Associates License Client PUTOLF Directory Traversal Vulnerability	2/22/05	3/2/05	8 days
407042	Computer Associates License Client PUTOLF Buffer Overflow Vulnerability	2/22/05	3/2/05	8 days
407040	Computer Associates License Client and Server Invalid Command Overflow Vulnerability	2/22/05	3/2/05	8 days
404904	RealNetworks RealPlayer .smil Buffer Overflow Vulnerability	1/13/05	3/1/05	47 days
404323	KPPP Local Privilege Escalation Vulnerability	2/2/05	2/28/05	26 days
404925	phpBB Group phpBB2 Arbitrary File Unlink Vulnerability	2/9/05	2/22/05	13 days
404924	phpBB Group phpBB Arbitrary File Disclosure Vulnerability	2/9/05	2/22/05	13 days
403205	ZoneAlarm 5.1 Invalid Pointer Dereference Vulnerability	1/4/05	2/11/05	38 days
403649	Openswan XAUTH/PAM Buffer Overflow Vulnerability	1/4/05	1/26/05	22 days
405736	DataRescue Interactive Disassembler Pro Buffer Overflow Vulnerability	1/10/05	1/24/05	14 days
403368	Multiple Unix/Linux Vendor Xpdf makeFileKey2 Stack Overflow	1/3/05	1/18/05	15 days
401617	SGI IRIX Local inpview Input Validation Vulnerability	1/3/05	1/13/05	10 days

+ For More Information

For more information about VeriSign® iDefense® Security Intelligence Services, please call 650.426.5310 or email enterprise_security@verisign.com.

Visit us at www.Verisign.com for more information.

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," TeraGuard, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.

11-01-2005