Vulnerability Summary for the Week of April 7, 2008

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered / Published	CVSS Score	Source & Patch Info
activepdf -- docconverter Symantec -- mail_security_appliance IBM -- Lotus Notes	Multiple buffer overflows in kpagrdr.dll 2.0.0.2 and 10.3.0.0 in the Applix Presents reader in Autonomy (formerly Verity) KeyView, as used by IBM Lotus Notes, Symantec Mail Security, and	unknown		CVE-2007-5405 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID

Autonomy -- KeyView Symantec -- Mail Security	activePDF DocConverter, allow remote attackers to execute arbitrary code via a .ag file with (1) a long ENCODING attribute in a *BEGIN tag, (2) a long token, or (3) the initial *BEGIN tag.	2008-04-10	9.3	FRSIRT FRSIRT FRSIRT SECTRACK SECUNIA SECUNIA SECUNIA SECUNIA SECUNIA
activepdf -- docconverter Symantec -- mail_security_appliance IBM -- Lotus Notes Autonomy -- KeyView Symantec -- Mail Security	Multiple stack-based buffer overflows in foliosr.dll in the Folio Flat File speed reader in Autonomy (formerly Verity) KeyView 10.3.0.0, as used by IBM Lotus Notes, Symantec Mail Security, and activePDF DocConverter, allow remote attackers to execute arbitrary code via a long attribute value in a (1) DI, (2) FD, (3) FT, (4) JD, (5) JL, (6) LE, (7) OB, (8) OD, (9) OL, (10) PN, (11) PS, (12) PW, (13) RD, (14) QL, or	unknown 2008-04-10	9.3	CVE-2007-6020 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID FRSIRT FRSIRT FRSIRT SECTRACK SECUNIA SECUNIA SECUNIA SECUNIA SECUNIA

	(15) TS tag in a .fff file.			
Adobe -- Flex Adobe -- AIR Adobe -- Flash Player	Adobe Flash Player 9.0.115.0 and earlier, and 8.0.39.0 and earlier, allows remote attackers to execute arbitrary code via an SWF file with a modified DeclareFunction2 Actionscript tag, which prevents an object from being instantiated properly.	unknown 2008-04-09	9.3	CVE-2007-6019 BUGTRAQ OTHER-REF OTHER-REF REDHAT BID SECTRACK
Adobe -- ColdFusion	Adobe ColdFusion 8 and 8.0.1 does not properly implement the public access level for CFC methods, which allows remote attackers to invoke these methods via Flex 2 remoting, a different vulnerability than CVE-2006-4725.	unknown 2008-04-09	7.5	CVE-2008-1656 OTHER-REF FRSIRT SECTRACK SECUNIA

CA -- threat_manager_for_the_enterprise CA -- Anti-Virus for the Enterprise CA -- BrightStor ARCserve Backup	Multiple stack-based buffer overflows in Computer Associates (CA) Alert Notification Service (Alert.exe) 8.1.586.0, 8.0.450.0, and 7.1.758.0, as used in multiple CA products including Anti-Virus for the Enterprise 7.1 through r11.1 and Threat Manager for the Enterprise 8.1 and r8, allow remote authenticated users to execute arbitrary code via crafted RPC requests.	unknown 2008-04-07	9.0	CVE-2007-4620 IDEFENSE BUGTRAQ OTHER-REF BID XF SECTRACK SECTRACK
Computer Associates -- Desktop Management Suite Computer Associates -- arcserve_backup_laptops_and_desktops	Buffer overflow in the LGServer service in CA ARCserve Backup for Laptops and Desktops r11.0 through r11.5, and Suite 11.1 and 11.2, allows remote attackers to execute arbitrary code via unspecified "command arguments."	unknown 2008-04-07	9.3	CVE-2008-1328 BUGTRAQ OTHER-REF BID XF SECTRACK

Computer Associates -- Desktop Management Suite Computer Associates -- arcserve_backup_laptops_and_desktops	Unspecified vulnerability in the NetBackup service in CA ARCserve Backup for Laptops and Desktops r11.0 through r11.5, and Suite 11.1 and 11.2, allows remote attackers to execute arbitrary commands, related to "insufficient verification of file uploads."	unknown 2008-04-07	10.0	CVE-2008-1329 BUGTRAQ OTHER-REF BID XF SECTRACK
desiquintans -- writers_block_cms	SQL injection vulnerability in permalink.php in Desi Quintans Writer's Block CMS 3.8a allows remote attackers to execute arbitrary SQL commands via the PostID parameter.	unknown 2008-04-08	7.5	CVE-2008-1699 BUGTRAQ BID SECUNIA

GNU -- m4	The (1) maketemp and (2) mkstemp builtin functions in GNU m4 before 1.4.11 do not quote their output when a file is created, which might allow context-dependent attackers to trigger a macro expansion, leading to unspecified use of an incorrect filename.	unknown 2008-04-09	7.5	CVE-2008-1687 MLIST MLIST MLIST MLIST SLACKWARE SECUNIA SECUNIA
GNU -- m4	Unspecified vulnerability in GNU m4 before 1.4.11 might allow context-dependent attackers to execute arbitrary code, related to improper handling of filenames specified with the -F option. NOTE: it is not clear when this issue crosses privilege boundaries.	unknown 2008-04-09	7.5	CVE-2008-1688 MLIST MLIST SLACKWARE SECUNIA SECUNIA

HP -- rx6600 HP -- rx2660 HP -- bl860c HP -- rx3600	Unspecified vulnerability in the embedded management console in HP iLO-2 Management Processors (iLO-2 MP), as used in Integrity Servers rx2660, rx3600, and rx6600, and Integrity Blade Server model bl860c, allows remote attackers to cause a denial of service via unknown vectors.	unknown 2008-04-08	7.8	CVE-2008-0711 BUGTRAQ HP BID FRSIRT SECUNIA SECTRACK
HP -- OpenView Network Node Manager	Stack-based buffer overflow in ovwparser.dll in HP OpenView Network Node Manager (OV NNM) 7.51 allows remote attackers to execute arbitrary code via a long URI in an HTTP request processed by ovas.exe, as demonstrated by a certain topology/homeBaseView request. NOTE: some of these details are	unknown 2008-04-08	10.0	CVE-2008-1697 MILW0RM OTHER-REF BID SECUNIA XF

	obtained from third party information.			
IBM -- Lotus Notes Autonomy -- KeyView	Multiple heap-based buffer overflows in emlsr.dll in the EML reader in Autonomy (formerly Verity) KeyView 10.3.0.0, as used by IBM Lotus Notes, allow remote attackers to execute arbitrary code via a long (1) To, (2) Cc, (3) Bcc, (4) From, (5) Date, (6) Subject, (7) Priority, (8) Importance, or (9) X-MSMail-Priority header; (10) a long string at the beginning of an RFC2047 encoded-word in a header; (11) a long text string in an RFC2047 encoded-word in a header; or (12) a long Subject header, related to creation of an associated filename.	unknown 2008-04-10	9.3	CVE-2007-5399 OTHER-REF OTHER-REF OTHER-REF BID FRSIRT FRSIRT SECUNIA SECUNIA

IBM -- Lotus Notes Autonomy -- KeyView	Multiple buffer overflows in htmsr.dll in the HTML speed reader in Autonomy (formerly Verity) KeyView, as used by IBM Lotus Notes 7.0.2 and 7.0.3, allow remote attackers to execute arbitrary code via an HTML document with (1) "large chunks of data," or a long URL in the (2) BACKGROUND attribute of a BODY element or (3) SRC attribute of an IMG element.	unknown 2008-04-10	9.3	CVE-2008-0066 OTHER-REF OTHER-REF BID FRSIRT FRSIRT SECUNIA SECUNIA SECUNIA
IBM -- Lotus Notes Autonomy -- KeyView	Buffer overflow in kvdocve.dll in the KeyView document viewing engine in Autonomy (formerly Verity) KeyView, as used by IBM Lotus Notes 7.0.2 and 7.0.3, allows remote attackers to execute arbitrary code via a long pathname, as	unknown 2008-04-10	9.3	CVE-2008-1101 OTHER-REF OTHER-REF BID FRSIRT FRSIRT SECUNIA SECUNIA SECUNIA

	demonstrated by a long SRC attribute of an IMG element in an HTML document.			
IBM -- AIX	Untrusted search path vulnerability in chnfsmnt in IBM AIX 6.1 allows local users to gain privileges via a modified PATH environment variable.	unknown 2008-04-09	7.2	CVE-2008-1710 AIXAPAR FRSIRT SECTRACK
IBM -- Lotus Notes Autonomy -- KeyView	Buffer overflow in mimesr.dll in Autonomy (formerly Verity) KeyView, as used in IBM Lotus Notes before 8.0, might allow user-assisted remote attackers to execute arbitrary code via an e-mail message with a crafted Text mail (MIME) attachment.	unknown 2008-04-10	9.3	CVE-2008-1718 OTHER-REF

interwoven -- worksite_web	Double free vulnerability in Web TransferCtrl Class 8,2,1,4 (iManFile.cab), as used in WorkSite Web 8.2 before SP1 P2, allows remote attackers to execute arbitrary code via JavaScript that sets the Server property to a string, then sets the string to null.	unknown 2008-04-08	9.3	CVE-2008-1617 OTHER-REF BID FRSIRT SECUNIA
interwoven -- worksite_web	The Web TransferCtrl Class 8,2,1,4 (iManFile.cab), as used in WorkSite Web 8.2 before SP1 P2, allows remote attackers to cause a denial of service (memory consumption) via a large number of SendNrlLink directives, which opens a separate window for each directive.	unknown 2008-04-08	9.3	CVE-2008-1700 OTHER-REF

Microsoft -- windows-nt	The (1) VBScript (VBScript.dll) and (2) JScript (JScript.dll) scripting engines 5.1 and 5.6, as used in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 and SP2, does not properly decode script, which allows remote attackers to execute arbitrary code via unknown vectors.	unknown 2008-04-08	9.3	CVE-2008-0083 MS BID FRSIRT SECTRACK SECUNIA
Microsoft -- windows-nt	The DNS client in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, and Vista uses predictable DNS transaction IDs, which allows remote attackers to spoof DNS responses.	unknown 2008-04-08	8.8	CVE-2008-0087 MS BID FRSIRT SECTRACK SECUNIA

Microsoft -- windows-nt	Heap-based buffer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, and Server 2008 allows remote attackers to execute arbitrary code via an EMF or WMF image file with a malformed header that triggers improper "integer calculations," aka "GDI Heap Overflow Vulnerability."	unknown 2008-04-08	9.3	CVE-2008-1083 MS BID FRSIRT SECTRACK SECUNIA XF
Microsoft -- windows-nt	Unspecified vulnerability in the kernel in Microsoft Windows 200 SP4, XP SP2, Server 2003 SP1 and SP2, Vista SP1, and Server 2008 allows local users to execute arbitrary code via unknown vectors related to improper input validation.	unknown 2008-04-08	7.2	CVE-2008-1084 MS BID FRSIRT SECTRACK SECUNIA

Microsoft -- Internet Explorer	Use after free vulnerability in Microsoft Internet Explorer 5.01 SP4, 6 through SP1, and 7 allows remote attackers to execute arbitrary code via a crafted data stream that triggers memory corruption, as demonstrated using an invalid MIME-type that does not have a registered handler.	unknown 2008-04-08	9.3	CVE-2008-1085 MS OTHER-REF BID FRSIRT SECTRACK SECUNIA
Microsoft -- Internet Explorer Microsoft -- windows-nt	The HxTocCtrl ActiveX control (hxvz.dll), as used in Microsoft Internet Explorer 5.01 SP4 and 6 SP1, in Windows XP SP2, Server 2003 SP1 and SP2, Vista SP1, and Server 2008, allows remote attackers to execute arbitrary code via malformed arguments, which triggers memory corruption.	unknown 2008-04-08	9.3	CVE-2008-1086 MS BID FRSIRT SECTRACK SECUNIA XF

Microsoft -- windows-nt	Stack-based buffer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, and Server 2008 allows remote attackers to execute arbitrary code via an EMF image file with crafted filename parameters, aka "GDI Stack Overflow Vulnerability."	unknown 2008-04-08	9.3	CVE-2008-1087 MS BID FRSIRT SECTRACK SECUNIA
Microsoft -- Project	Microsoft Project 2000 Service Release 1, 2002 SP1, and 2003 SP2 allows user-assisted remote attackers to execute arbitrary code via a crafted Project file, related to improper validation of "memory resource allocations."	unknown 2008-04-08	9.3	CVE-2008-1088 MS CERT-VN BID FRSIRT SECTRACK SECUNIA XF

Microsoft -- Visio Microsoft -- Office	Unspecified vulnerability in Microsoft Visio 2002 SP2, 2003 SP2 and SP3, and 2007 up to SP1 allows user-assisted remote attackers to execute arbitrary code via a Visio file containing crafted object header data, aka "Visio Object Header Vulnerability."	unknown 2008-04-08	9.3	CVE-2008-1089 MS SECUNIA BID FRSIRT SECTRACK XF
Microsoft -- Visio Microsoft -- Office	Unspecified vulnerability in Microsoft Visio 2002 SP2, 2003 SP2 and SP3, and 2007 up to SP1 allows user-assisted remote attackers to execute arbitrary code via a crafted .DXF file, aka "Visio Memory Validation Vulnerability."	unknown 2008-04-08	9.3	CVE-2008-1090 MS BID SECUNIA FRSIRT SECTRACK XF

Microsoft -- Visual InterDev	Buffer overflow in Microsoft Visual InterDev 6.0 (SP6) allows user-assisted attackers to execute arbitrary code via a Studio Solution (.SLN) file with a long malformed Project line beginning with a 'Project("{}") =' sequence, probably a different vector than CVE-2008-0250.	unknown 2008-04-09	9.3	CVE-2008-1709 MILW0RM
Python Software Foundation -- Python	Integer signedness error in the zlib extension module in Python 2.5.2 and earlier allows remote attackers to execute arbitrary code via a negative signed integer, which triggers insufficient memory allocation and a buffer overflow.	unknown 2008-04-10	7.5	CVE-2008-1721 BUGTRAQ OTHER-REF BID

Samba -- rsync	Buffer overflow in rsync 2.6.9 to 3.0.1, with extended attribute (xattr) support enabled, might allow remote attackers to execute arbitrary code via unknown vectors.	unknown 2008-04-10	7.5	CVE-2008-1720 OTHER-REF OTHER-REF
Seattle Lab Software -- SLMail Pro	Stack consumption vulnerability in WebContainer.exe 1.0.0.336 and earlier in SLMail Pro 6.3.1.0 and earlier allows remote attackers to cause a denial of service (daemon crash) via a long request header in an HTTP request to TCP port 801. NOTE: some of these details are obtained from third party information.	unknown 2008-04-07	7.5	CVE-2008-1689 OTHER-REF OTHER-REF BID FRSIRT SECUNIA XF

Seattle Lab Software -- SLMail Pro	WebContainer.exe 1.0.0.336 and earlier in SLMail Pro 6.3.1.0 and earlier allows remote attackers to cause a denial of service (memory corruption and daemon crash) or possibly execute arbitrary code via a long URI in HTTP requests to TCP port 801. NOTE: some of these details are obtained from third party information.	unknown 2008-04-07	10.0	CVE-2008-1690 OTHER-REF BID FRSIRT SECUNIA XF
Symantec -- norton_360 Symantec -- Norton Internet Security Symantec -- Norton System Works Symantec -- Norton Antivirus	Stack-based buffer overflow in the AutoFix Support Tool ActiveX control 2.7.0.1 in SYMADATA.DLL in multiple Symantec Norton products, including Norton 360 1.0, AntiVirus 2006 through 2008, Internet Security 2006 through 2008, and System Works 2006 through 2008, allows	unknown 2008-04-08	9.3	CVE-2008-0312 IDEFENSE OTHER-REF BID FRSIRT SECTRACK SECTRACK

	remote attackers to execute arbitrary code via a long argument to the GetEventLogInfo method. NOTE: some of these details are obtained from third party information.			SECTRACK SECUNIA
Tibco -- Enterprise Message Service Tibco -- iprocess_engine	Multiple buffer overflows in TIBCO Software Enterprise Message Service (EMS) before 4.4.3, and iProcess Engine 10.6.0 through 10.6.1, allow remote attackers to execute arbitrary code via a crafted message to the EMS server.	unknown 2008-04-11	10.0	CVE-2008-1704 OTHER-REF BID SECUNIA
Tumbleweed -- securetransport_server_app	Stack-based buffer overflow in the IActiveXTransfer.FileTransfer method in the SecureTransport FileTransfer ActiveX control in vcst_en.dll 1.0.0.5 in Tumbleweed SecureTransport Server before	unknown 2008-04-11	9.3	CVE-2008-1724 BUGTRAQ MILW0RM OTHER-REF BID FRSIRT

	4.6.1 Hotfix 20 allows remote attackers to execute arbitrary code via a long remoteFile parameter.			SECUNIA XF

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Adobe -- Flex Adobe -- AIR Adobe -- Flash Player	Unspecified vulnerability in Adobe Flash Player 9.0.115.0 and earlier, and 8.0.39.0 and earlier, allows remote attackers to execute arbitrary code via unknown vectors related to "input validation errors."	unknown 2008-04-09	6.8	CVE-2007-0071 OTHER-REF REDHAT
Adobe -- Flex Adobe -- AIR Adobe -- Flash Player	Unspecified vulnerability in Adobe Flash Player 9.0.115.0 and earlier, and 8.0.39.0 and earlier, makes it easier for remote attackers to conduct DNS rebinding attacks via unknown vectors.	unknown 2008-04-09	4.3	CVE-2008-1655 OTHER-REF OTHER-REF REDHAT BID
auraCMS -- AuraCMS	SQL injection vulnerability in content/user.php in AuraCMS 2.2.1 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the country parameter.	unknown 2008-04-09	6.8	CVE-2008-1715 MILW0RM BID SECUNIA XF

cups -- CUPS	Multiple integer overflows in (1) filter/image-png.c and (2) filter/image-zoom.c in CUPS 1.3 allow attackers to cause a denial of service (crash) and trigger memory corruption, as demonstrated via a crafted PNG image.	unknown 2008-04-10	4.3	CVE-2008-1722 OTHER-REF
dazphp -- dazphpnews	Directory traversal vulnerability in makepost.php in DaZPHPNews 0.1-1, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the prefixdir parameter.	unknown 2008-04-08	4.4	CVE-2008-1696 MILW0RM BID SECUNIA
e107 -- e107	Absolute path traversal vulnerability in dload.php in the my_gallery 2.3 plugin for e107 allows remote attackers to obtain sensitive information via a full pathname in the file parameter. NOTE: some of these details are obtained from third party information.	unknown 2008-04-08	5.0	CVE-2008-1702 BUGTRAQ MILW0RM BID SECUNIA
eterm -- eterm	Eterm 0.9.4 opens an xterm on :0 if -display is not specified and the DISPLAY environment variable is not set, which might allow local users to hijack X11 connections.	unknown 2008-04-07	6.9	CVE-2008-1692 OTHER-REF SECUNIA

FaScript -- Faphoto	SQL injection vulnerability in show.php in FaScript FaPhoto 1.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-04-09	6.8	CVE-2008-1714 MILW0RM BID SECUNIA XF
HP -- Select Identity	Multiple unspecified vulnerabilities in HP Select Identity 4.00, 4.01, 4.11, 4.12, 4.13, and 4.20 allow remote authenticated users to access other user accounts via unknown vectors, a different issue than CVE-2008-0214.	unknown 2008-04-07	6.8	CVE-2008-0709 HP BID FRSIRT SECTRACK SECUNIA
IBM -- Lotus Notes Autonomy -- KeyView Symantec -- Mail Security	kpagrdr.dll 2.0.0.2 and 10.3.0.0 in the Applix Presents reader in Autonomy (formerly Verity) KeyView, as used by IBM Lotus Notes, Symantec Mail Security, and activePDF DocConverter, does not properly parse long tokens, which allows remote attackers to cause a denial of service (CPU and memory consumption) via a crafted .ag file.	unknown 2008-04-10	4.3	CVE-2007-5406 OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID FRSIRT FRSIRT FRSIRT SECTRACK SECUNIA SECUNIA SECUNIA SECUNIA SECUNIA

IBM -- solidDB	Format string vulnerability in the logging function in IBM solidDB 06.00.1018 and earlier allows remote attackers to execute arbitrary code via format string specifiers in the (1) user name, (2) peer name, and possibly unspecified other fields.	unknown 2008-04-09	6.8	CVE-2008-1705 OTHER-REF OTHER-REF FRSIRT SECTRACK
IBM -- solidDB	Uncontrolled array index in IBM solidDB 06.00.1018 and earlier allows remote attackers to cause a denial of service (daemon crash) via a large value in a certain 32-bit field.	unknown 2008-04-09	4.3	CVE-2008-1706 OTHER-REF OTHER-REF FRSIRT SECTRACK
IBM -- solidDB	IBM solidDB 06.00.1018 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a packet with an 0x11 value in a certain "type" field.	unknown 2008-04-09	4.3	CVE-2008-1707 OTHER-REF OTHER-REF FRSIRT SECTRACK
IBM -- solidDB	IBM solidDB 06.00.1018 and earlier does not validate a certain field that specifies an amount of memory to allocate, which allows remote attackers to cause a denial of service (daemon exit) via a packet with a large value in this field.	unknown 2008-04-09	4.3	CVE-2008-1708 OTHER-REF OTHER-REF FRSIRT SECTRACK

mx_system -- mxBB	PHP remote file inclusion vulnerability in includes/functions_weblog.php in mxbBB mx_blogs 2.0.0 beta allows remote attackers to execute arbitrary PHP code via a URL in the mx_root_path parameter.	unknown 2008-04-09	6.8	CVE-2008-1712 MILW0RM BID
noticeware -- email_server	MailServer.exe in NoticeWare Email Server 4.6.1.0 allows remote attackers to cause a denial of service (application crash) via a long string to IMAP port (143/tcp).	unknown 2008-04-09	5.0	CVE-2008-1713 MILW0RM BID SECUNIA
Novell -- iPrint	Novell NetWare 6.5 allows attackers to cause a denial of service (ABEND) via a crafted Macintosh iPrint client request.	unknown 2008-04-08	5.0	CVE-2008-1701 OTHER-REF SECUNIA
redhat -- policykit	Format string vulnerability in the grant helper (polkit-grant-helper.c) in PolicyKit 0.7 and earlier allows attackers to cause a denial of service (crash) and possibly execute arbitrary code via format strings in a password.	unknown 2008-04-11	6.9	CVE-2008-1658 OTHER-REF OTHER-REF OTHER-REF FEDORA SECUNIA
rxvt -- Rxvt	rxvt 2.6.4 opens an xterm on :0 if the DISPLAY environment variable is not set, which might allow local users to hijack X11 connections.	unknown 2008-04-07	4.6	CVE-2008-1142 OTHER-REF OTHER-REF SECUNIA

SCO -- UnixWare	Directory traversal vulnerability in pkgadd in SCO UnixWare 7.1.4 before p534589 allows local users to create or append to arbitrary files via ".." sequences in an unspecified environment variable, probably PKGINST.	unknown 2008-04-07	6.9	CVE-2008-0310 IDEFENSE MILW0RM SCO SECTRACK SECUNIA
Seattle Lab Software -- SLMail Pro	Unspecified vulnerability in SLMail.exe in SLMail Pro 6.3.1.0 and earlier allows remote attackers to cause a denial of service (UDP service outage) via a large packet to UDP port 54. NOTE: some of these details are obtained from third party information.	unknown 2008-04-07	5.0	CVE-2008-1691 OTHER-REF BID FRSIRT SECUNIA XF
Symantec -- norton_360 Symantec -- system_works Symantec -- Norton Internet Security Symantec -- Norton Antivirus	The ActiveDataInfo.LaunchProcess method in the SymAData.ActiveDataInfo.1 ActiveX control 2.7.0.1 in SYMADATA.DLL in multiple Symantec Norton products including Norton 360 1.0, AntiVirus 2006 through 2008, Internet Security 2006 through 2008, and System Works 2006 through 2008, does not properly determine the location of the AutoFix Tool, which allows remote attackers to execute arbitrary code via a remote (1) WebDAV or (2) SMB share.	unknown 2008-04-08	6.8	CVE-2008-0313 IDEFENSE OTHER-REF BID FRSIRT SECTRACK SECTRACK SECTRACK SECUNIA

Terong -- advanced_web_photo_gallery	Terong PHP Photo Gallery (aka Advanced Web Photo Gallery) 1.0 stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information.	unknown 2008-04-09	5.0	CVE-2008-1711 MILW0RM SECUNIA
Tibco -- rendezvous_datasecurity Tibco -- Runtime Agent Tibco -- adapter_files_z_os Tibco -- rendezvous_tx Tibco -- substantiation_es Tibco -- Hawk Tibco -- iprocess_engine Tibco -- Rendezvous	Multiple buffer overflows in TIBCO Software Rendezvous before 8.1.0, as used in multiple TIBCO products, allow remote attackers to execute arbitrary code via a crafted message.	unknown 2008-04-11	6.8	CVE-2008-1703 OTHER-REF BID SECUNIA
Tru-Zone -- NukeET	Multiple cross-site request forgery (CSRF) vulnerabilities in Nuke ET 3.2 and 3.4 allow remote attackers to perform actions as administrators, as demonstrated by inserting an XSS sequence into a document.	unknown 2008-04-10	4.3	CVE-2008-1719 OTHER-REF SECUNIA
ventrian -- simple_gallery	Cross-site scripting (XSS) vulnerability in gallery.php in Simple Gallery 2.2 allows remote attackers to inject arbitrary web script or HTML via the album parameter to index.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-08	4.3	CVE-2008-1698 SECUNIA

WatchGuard -- Firebox_PPTP_VPN	The PPTP VPN service in Watchguard Firebox before 10, when performing the MS-CHAPv2 authentication handshake, generates different error codes during depending on whether the username is valid or invalid, which allows remote attackers to enumerate valid usernames.	unknown 2008-04-07	5.0	CVE-2008-1618 OTHER-REF BID SECTRACK
WoltLab -- Burning Board	Cross-site scripting (XSS) vulnerability in WoltLab Community Framework (WCF) 1.0.6 in WoltLab Burning Board 3.0.5 allows remote attackers to inject arbitrary web script or HTML via the (1) page and (2) form parameters, which are not properly handled when they are reflected back in an error message.	unknown 2008-04-09	4.3	CVE-2008-1716 FULLDISC SECUNIA
WoltLab -- Burning Board	WoltLab Community Framework (WCF) 1.0.6 in WoltLab Burning Board 3.0.5 allows remote attackers to obtain the full path via invalid (1) page and (2) form parameters, which leaks the path from an exception handler when a valid class cannot be found.	unknown 2008-04-09	5.0	CVE-2008-1717 FULLDISC SECUNIA

Xiph.Org -- libfishsound	Uncontrolled array index in Speex 1.1.12 and earlier, as used in libfishsound 0.9.0 and earlier, including Illiminable DirectShow Filters and Annodex Plugins for Firefox, allows remote attackers to execute arbitrary code via a header structure containing a negative offset, which is used to dereference a function pointer.	unknown 2008-04-08	6.8	CVE-2008-1686 MLIST OTHER-REF OTHER-REF BID SECUNIA XF

Back to top

There were no low vulnerabilities recorded this week.

Last updated April 14, 2008