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
	SQL injection vulnerability in view_ann.php in Vastal I-Tech Agent Zone (aka The Real Estate Script) allows remote attackers to execute arbitrary SQL commands via the ann_id parameter.	2008-09-10	7.5	CVE-2008-3951 BID MILW0RM
	SQL injection vulnerability in questions.php in EsFaq 2.0 allows remote attackers to execute arbitrary SQL commands via the idcat parameter.	2008-09-10	7.5	CVE-2008-3952
	SQL injection vulnerability in index.php in AlstraSoft Forum Pay Per Post Exchange allows remote attackers to execute arbitrary SQL commands via the cat parameter in a showcat action.	2008-09-10	7.5	CVE-2008-3954

	The Microsoft Windows Image Acquisition Logger ActiveX control allows remote attackers to force the download of arbitrary files onto a client system via a URL in the first argument to the Open method, in conjunction with a full destination pathname in the first argument to the Save method. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-09-10	9.3	CVE-2008-3957
	SQL injection vulnerability in index.php in Spice Classifieds allows remote attackers to execute arbitrary SQL commands via the cat_path parameter.	2008-09-11	7.5	CVE-2008-4039
	Directory traversal vulnerability in the Kyocera Command Center in Kyocera FS-118MFP allows remote attackers to read arbitrary files via a .. (dot dot) in the URI.	2008-09-11	7.8	CVE-2008-4040
	SQL injection vulnerability in tops_top.php in Million Pixel Ad Script (Million Pixel Script) allows remote attackers to execute arbitrary SQL commands via the id_cat parameter.	2008-09-11	7.5	CVE-2008-4055
aj_square -- aj_hyip	Multiple SQL injection vulnerabilities in AJ Square AJ HYIP Acme allow remote attackers to execute arbitrary SQL commands via the artid parameter to (1) acme/article/comment.php or (2) prime/article/comment.php.	2008-09-11	7.5	CVE-2008-4043
aj_square -- aj_hyip	SQL injection vulnerability in article/readarticle.php in AJ Square aj-hyip (aka AJ HYIP Acme) allows remote attackers to execute arbitrary SQL commands via the artid parameter.	2008-09-11	7.5	CVE-2008-4044
apple -- ipod_touch	The Networking subsystem in Apple iPod touch 2.0 through 2.0.2 uses predictable TCP initial sequence numbers, which allows remote attackers to spoof or hijack a TCP connection.	2008-09-10	7.5	CVE-2008-3612

apple -- quicktime	Stack-based buffer overflow in Apple QuickTime before 7.5.5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a QuickTime Virtual Reality (QTVR) movie file with crafted (1) maxTilt, (2) minFieldOfView, and (3) maxFieldOfView elements in panorama track PDAT atoms.	2008-09-10	10.0	CVE-2008-3625 BID CONFIRM
apple -- quicktime	Apple QuickTime before 7.5.5 does not properly handle (1) MDAT atoms in MP4 video files within QuickTimeH264.qtx, (2) MDAT atoms in mov video files within QuickTimeH264.scalar, and (3) AVC1 atoms in an unknown media type within an unspecified component, which allows remote attackers to execute arbitrary code or cause a denial of service (heap corruption and application crash) via a crafted, H.264 encoded movie file.	2008-09-10	9.3	CVE-2008-3627 BID
apple -- quicktime	Apple QuickTime before 7.5.5 on Windows allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PICT image, related to an "invalid pointer issue."	2008-09-10	9.3	CVE-2008-3628 BID CONFIRM
apple -- ipod_touch	Application Sandbox in Apple iPod touch 2.0 through 2.0.2 does not properly isolate third-party applications, which allows attackers to read arbitrary files in a third-party application's sandbox via a different third-party application.	2008-09-10	7.1	CVE-2008-3631
apple -- ipod_touch	Use-after-free vulnerability in WebKit in Apple iPod touch 1.1 through 2.0.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a web page with crafted Cascading Style Sheets (CSS) import statements.	2008-09-10	9.3	CVE-2008-3632
apple -- quicktime intel -- indeo	Stack-based buffer overflow in QuickTimeInternetExtras.qtx in an unspecified third-party Indeo v3.2	2008-09-10	9.3	CVE-2008-3635

	(aka IV32) codec for QuickTime, when used with Apple QuickTime before 7.5.5 on Windows, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted movie file.			
apple -- itunes	Integer overflow in an unspecified third-party driver bundled with Apple iTunes before 8.0 on Windows allows local users to gain privileges via unknown vectors.	2008-09-10	7.2	CVE-2008-3636 BID
bitlbee -- bitlbee	Multiple unspecified vulnerabilities in BitlBee before 1.2.3 allow remote attackers to "overwrite" and "hijack" existing accounts via unknown vectors. NOTE: this issue exists because of an incomplete fix for CVE-2008-3920.	2008-09-10	7.5	CVE-2008-3969
clam_anti-virus -- clamav	Multiple unspecified vulnerabilities in ClamAV before 0.94 have unknown impact and attack vectors related to file descriptor leaks on the "error path" in (1) libclamav/others.c and (2) libclamav/sis.c.	2008-09-10	10.0	CVE-2008-3914 BID CONFIRM
elitecms -- elitecms	SQL injection vulnerability in index.php in eliteCMS 1.0 allows remote attackers to execute arbitrary SQL commands via the page parameter.	2008-09-11	7.5	CVE-2008-4046
friendly_technologies -- friendly_pppoe_client	A certain ActiveX control in fwRemoteCfg.dll 3.3.3.1 in Friendly Technologies FriendlyPPPoE Client 3.0.0.57 allows remote attackers to (1) create and read arbitrary registry values via the RegistryValue method, and (2) read arbitrary files via the GetTextFile method.	2008-09-11	9.3	CVE-2008-4050
gmanedit2 -- gmanedit	Heap-based buffer overflow in the open_man_file function in callbacks.c in gmanedit 0.4.1 allows remote attackers to execute arbitrary code via a crafted man page, which is not properly handled during utf8 conversion. NOTE: another overflow was reported using a configuration file, but that vector does not have a	2008-09-10	9.3	CVE-2008-3971

	scenario that crosses privilege boundaries.			
hp -- openvms	Stack-based buffer overflow in SMGSHR.EXE in OpenVMS for Integrity Servers 8.2-1, 8.3, and 8.3-1H1 and OpenVMS ALPHA 7.3-2, 8.2, and 8.3 allows local users to cause a denial of service (crash) or gain privileges via unspecified vectors.	2008-09-11	7.2	CVE-2008-4052 FRSIRT MLIST MLIST MLIST MLIST MLIST MLIST
ibm -- aix	Buffer overflow in tftp in bos.net.tcp.client in IBM AIX 5.2.0 and 5.3.0 allows local users to gain privileges via unspecified vectors.	2008-09-10	7.2	CVE-2007-6717 CONFIRM SECUNIA
ibm -- db2	IBM DB2 UDB 8 before Fixpak 17 allows remote attackers to cause a denial of service (instance crash) via a crafted CONNECT/ATTACH data stream that simulates a V7 client connect/attach request. NOTE: this may overlap CVE-2008-3858. NOTE: this issue exists because of an incomplete fix for CVE-2008-3959.	2008-09-10	10.0	CVE-2008-3958
ibm -- aix	swcons in bos.rte.console in IBM AIX 5.2.0 through 6.1.1 allows local users in the system group to create or overwrite an arbitrary file, and establish weak permissions and root ownership for this file, via unspecified vectors. NOTE: this can be leveraged to gain privileges. NOTE: this issue exists because of an incomplete fix for CVE-2007-5805.	2008-09-10	7.2	CVE-2008-4018
kolifa -- download_script	SQL injection vulnerability in indir.php in Kolifa.net Download Script 1.2 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-09-11	7.5	CVE-2008-4054
linux -- kernel	Buffer overflow in nfsd in the Linux kernel before 2.6.26.4, when NFSv4 is enabled, allows remote attackers to have an unknown impact via vectors related to decoding an NFSv4 acl.	2008-09-10	9.3	CVE-2008-3915

masir_camp -- e-shop_module	SQL injection vulnerability in index.php in Masir Camp E-Shop Module 3.0 and earlier allows remote attackers to execute arbitrary SQL commands via the ordercode parameter in a veiworderstatus page.	2008-09-10	7.5	CVE-2008-3955
microsoft -- digital_image_suite microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_powerpoint_viewer microsoft -- report_viewer microsoft -- server microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- works microsoft -- office_system microsoft -- windows microsoft -- windows-nt	Heap-based buffer overflow in the vector graphics link library in gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via an image file with crafted gradient sizes, aka "GDI+ VML Buffer Overrun Vulnerability."	2008-09-10	9.3	CVE-2007-5348
microsoft -- windows_media_player	Unspecified vulnerability in Microsoft Windows Media Player 11 allows remote attackers to execute arbitrary code via a crafted audio-only file that is streamed from a Server-Side Playlist (SSPL) on Windows Media Server, aka "Windows Media Player Sampling Rate Vulnerability."	2008-09-10	9.3	CVE-2008-2253
microsoft -- windows_media_encoder microsoft -- windows-nt	Buffer overflow in a certain ActiveX control in wmex.dll in Microsoft Windows Media Encoder 9 Series allows remote attackers to execute arbitrary code via unspecified vectors, aka "Windows Media Encoder Buffer Overrun Vulnerability."	2008-09-10	9.3	CVE-2008-3008 MS
microsoft -- digital_image_suite microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office	gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office	2008-09-10	9.3	CVE-2008-3012 MS

microsoft -- office_powerpoint_viewer microsoft -- report_viewer microsoft -- server microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- works microsoft -- office_system microsoft -- windows microsoft -- windows-nt	System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 does not properly perform memory allocation, which allows remote attackers to execute arbitrary code via a malformed EMF image file, aka "GDI+ EMF Memory Corruption Vulnerability."			
microsoft -- digital_image_suite microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_powerpoint_viewer microsoft -- report_viewer microsoft -- server microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- works microsoft -- office_system microsoft -- windows microsoft -- windows-nt	gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 does not properly parse records in a GIF image file, which allows remote attackers to execute arbitrary code via a malformed GIF file, aka "GDI+ GIF Parsing Vulnerability."	2008-09-10	9.3	CVE-2008-3013
microsoft -- digital_image_suite microsoft -- forefront_client_security microsoft -- internet_explorer microsoft -- office microsoft -- office_powerpoint_viewer microsoft -- report_viewer microsoft -- server microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- works microsoft -- server microsoft -- windows-nt	Buffer overflow in gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a malformed WMF image file that triggers improper memory allocation, aka "GDI+ WMF Buffer	2008-09-10	9.3	CVE-2008-3014

	Overrun Vulnerability."			
microsoft -- digital_image_suite microsoft -- forefront_client_security microsoft -- office microsoft -- office_powerpoint_viewer microsoft -- report_viewer microsoft -- sql_server microsoft -- sql_server_reporting_services microsoft -- visio microsoft -- works	Integer overflow in gdiplus.dll in GDI+ in Microsoft Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted BMP image file with a malformed header that triggers a buffer overflow, aka "GDI+ BMP Integer Overflow Vulnerability."	2008-09-10	9.3	CVE-2008-3015 MS
microsoft -- organization_chart	orgchart.exe in Microsoft Organization Chart 2.00 allows user-assisted attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted .opx file.	2008-09-10	9.3	CVE-2008-3956
mybb -- mybb	SQL injection vulnerability in misc.php in MyBB (aka MyBulletinBoard) before 1.4.1 allows remote attackers to execute arbitrary SQL commands via a certain editor field.	2008-09-10	7.5	CVE-2008-3965
mybb -- mybb	moderation.php in MyBB (aka MyBulletinBoard) before 1.4.1 does not properly check for moderator privileges, which has unknown impact and remote attack vectors.	2008-09-10	7.5	CVE-2008-3967
netbsd -- netbsd	The mld_input function in sys/netinet6/mld6.c in the kernel in NetBSD 4.0, FreeBSD, and KAME, when INET6 is enabled, allows remote attackers to cause a denial of service (divide-by-zero error and panic) via a malformed ICMPv6 Multicast Listener Discovery (MLD) query with a certain Maximum Response Delay value.	2008-09-10	7.1	CVE-2008-2464
netbsd -- netbsd	NetBSD 3.0, 3.1, and 4.0, when a pppoe instance exists, does not properly check the length of a PPPoE	2008-09-11	9.3	CVE-2008-3584

	packet tag, which allows remote attackers to cause a denial of service (system crash) via a crafted PPPoE packet.			
novell -- novell_forum	Unspecified vulnerability in Novell Forum (formerly SiteScape Forum) 7.0, 7.1, 7.2, 7.3, and 8.0 allows remote attackers to execute arbitrary TCL code via a modified URL. NOTE: this might overlap CVE-2007-6515.	2008-09-11	7.5	CVE-2008-4047 CONFIRM
objective_development -- sharity	Unspecified vulnerability in Objective Development Sharity 3 before 3.5 has unknown impact and attack vectors, related to a "serious security problem."	2008-09-11	10.0	CVE-2008-4057
redhat -- adminutil	Heap-based buffer overflow in Red Hat adminutil 1.1.6 allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via % (percent) encoded HTTP input to unspecified CGI scripts in Fedora Directory Server. NOTE: this vulnerability exists because of an incorrect fix for CVE-2008-2929.	2008-09-12	10.0	CVE-2008-2932
redhat -- freeipa redhat -- ipa	The default configuration of Red Hat Enterprise IPA 1.0.0 and FreeIPA before 1.1.1 places ldap:///anyone on the read ACL for the krbMKey attribute, which allows remote attackers to obtain the Kerberos master key via an anonymous LDAP query.	2008-09-12	10.0	CVE-2008-3274 CONFIRM
vastal -- shaadi_zone	SQL injection vulnerability in keyword_search_action.php in Vastal I-Tech Shaadi Zone 1.0.9 allows remote attackers to execute arbitrary SQL commands via the tage parameter.	2008-09-10	7.5	CVE-2008-3953
xmlsoft -- libxml2 redhat -- desktop redhat -- desktop_workstation redhat -- enterprise_linux redhat -- enterprise_linux_desktop redhat --	Heap-based buffer overflow in the xmlParseAttValueComplex function in parser.c in libxml2 before 2.7.0 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long XML entity name.	2008-09-12	10.0	CVE-2008-3529

linux_advanced_workstation

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
	MySQL 5.0 before 5.0.66, 5.1 before 5.1.26, and 6.0 before 6.0.6 does not properly handle a b'' (b single-quote single-quote) token, aka an empty bit-string literal, which allows remote attackers to cause a denial of service (daemon crash) by using this token in a SQL statement.	2008-09-10	5.0	CVE-2008-3963
@mail -- @mail	Multiple cross-site scripting (XSS) vulnerabilities in @Mail 5.42 allow remote attackers to inject arbitrary web script or HTML via the (1) file and (2) HelpFile parameters to parse.php, the (3) Folder and (4) start parameters to showmail.php, and the (5) abookview parameter to abook.php.	2008-09-11	4.3	CVE-2008-4045
apple -- bonjour	mDNSResponder in the Bonjour Namespace Provider in Apple Bonjour for Windows before 1.0.5 allows attackers to cause a denial of service (NULL pointer dereference and application crash) by resolving a crafted .local domain name that contains a long label.	2008-09-10	5.0	CVE-2008-2326 BID
apple -- quicktime apple -- mac_os_x apple -- mac_os_x_server microsoft -- windows-nt	Integer overflow in Apple QuickTime before 7.5.5 on Windows allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PICT image, which triggers heap corruption.	2008-09-10	6.8	CVE-2008-3614
apple -- quicktime apple -- mac_os_x microsoft -- windows-nt	Heap-based buffer overflow in Apple QuickTime before 7.5.5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a QuickTime Virtual Reality (QTVR) movie file with crafted panorama atoms.	2008-09-10	6.8	CVE-2008-3624
apple -- quicktime	The CallComponentFunctionWithStorage function in Apple QuickTime before 7.5.5 does not properly handle a large entry in the sample_size_table in STSZ atoms, which allows remote attackers to execute	2008-09-10	6.8	CVE-2008-3626 MISC BID CONFIRM SECTRACK

	arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file.			
apple -- quicktime apple -- mac_os_x apple -- mac_os_x_server microsoft -- windows-nt	Apple QuickTime before 7.5.5 allows remote attackers to cause a denial of service (application crash) via a crafted PICT image that triggers an out-of-bounds read.	2008-09-10	6.8	CVE-2008-3629 APPLE
apple -- bonjour	mDNSResponder in Apple Bonjour for Windows before 1.0.5, when an application uses the Bonjour API for unicast DNS, does not choose random values for transaction IDs or source ports in DNS requests, which makes it easier for remote attackers to spoof DNS responses, a different vulnerability than CVE-2008-1447.	2008-09-10	6.4	CVE-2008-3630 APPLE
bluemoon -- popnupblog	Multiple cross-site scripting (XSS) vulnerabilities in index.php in the Bluemoon PopnupBLOG module 3.20 and 3.30 for XOOPS allow remote attackers to inject arbitrary web script or HTML via the (1) param, (2) cat_id, and (3) view parameters.	2008-09-11	4.3	CVE-2008-4053
clam_anti-virus -- clamav	libclamav in ClamAV before 0.94 allows attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors related to an out-of-memory condition.	2008-09-10	5.0	CVE-2008-3912 BID CONFIRM
clam_anti-virus -- clamav	Multiple memory leaks in freshclam/manager.c in ClamAV before 0.94 might allow attackers to cause a denial of service (memory consumption) via unspecified vectors related to the "error path."	2008-09-10	5.0	CVE-2008-3913 BID
friendly_technologies -- friendly_pppoe_client	Heap-based buffer overflow in a certain ActiveX control in fwRemoteCfg.dll 3.3.3.1 in Friendly Technologies FriendlyPPPoE Client 3.0.0.57 allows remote attackers to execute arbitrary code via a long third argument to the CreateURLShortcut method.	2008-09-11	6.8	CVE-2008-4048
friendly_technologies -- friendly_pppoe_client	A certain ActiveX control in fwRemoteCfg.dll 3.3.3.1 in Friendly Technologies FriendlyPPPoE Client	2008-09-11	6.8	CVE-2008-4049

	3.0.0.57 allows remote attackers to execute arbitrary programs via arguments to the RunApp method.			
horde -- horde	Cross-site scripting (XSS) vulnerability in MIME/MIME/Contents.php in the MIME library in Horde 3.2.x before 3.2.2 allows remote attackers to inject arbitrary web script or HTML via the filename of a MIME attachment in an e-mail message.	2008-09-12	4.3	CVE-2008-3823 BUGTRAQ MLIST MISC MLIST
horde -- horde popoon -- popoon	Cross-site scripting (XSS) vulnerability in (1) Text_Filter/Filter/xss.php in Horde 3.1.x before 3.1.9 and 3.2.x before 3.2.2 and (2) externalinput.php in Popoon r22196 and earlier allows remote attackers to inject arbitrary web script or HTML by using / (slash) characters as replacements for spaces in an HTML e-mail message.	2008-09-12	4.3	CVE-2008-3824 BUGTRAQ MISC MISC MISC MLIST
ibm -- db2	IBM DB2 UDB 8.1 before FixPak 16, and 8.2 before FixPak 9, allows remote attackers to cause a denial of service (instance crash) via a crafted CONNECT/ATTACH data stream that simulates a V7 client connect/attach request.	2008-09-10	5.0	CVE-2008-3959 AIXAPAR
ibm -- db2_universal_database	Unspecified vulnerability in the JDBC Applet Server Service (aka db2jds) in IBM DB2 UDB 8 before Fixpak 17 allows remote attackers to cause a denial of service (service crash) via "malicious packets."	2008-09-10	5.0	CVE-2008-3960
jandus_technologies -- smart_survey	Cross-site scripting (XSS) vulnerability in surveyresults.asp in Smart Survey 1.0 allows remote attackers to inject arbitrary web script or HTML via the sid parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-09-11	4.3	CVE-2008-4051
libpng -- libpng	Multiple off-by-one errors in libpng before 1.2.32beta01, and 1.4 before 1.4.0beta34, allow context-dependent attackers to cause a denial of service (crash) or have unspecified other impact via a PNG image with crafted zTXt chunks, related to (1) the png_push_read_zTXt function in pngread.c, and possibly related to (2) pngtest.c.	2008-09-10	4.3	CVE-2008-3964 CONFIRM

matterdaddy -- matterdaddy_market	Cross-site scripting (XSS) vulnerability in admin/login.php in Matterdaddy Market 1.1 allows remote attackers to inject arbitrary web script or HTML via the msg parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-09-11	4.3	CVE-2008-4056
microsoft -- office microsoft -- office_onenote	Microsoft Office XP SP3, 2003 SP2 and SP3, 2007 Office System Gold and SP1, and Office OneNote 2007 Gold and SP1 allow remote attackers to execute arbitrary code via a crafted onenote:// URL, aka "Uniform Resource Locator Validation Error Vulnerability."	2008-09-10	6.8	CVE-2008-3007
mybb -- mybb	Multiple cross-site scripting (XSS) vulnerabilities in MyBB (aka MyBulletinBoard) before 1.4.1 allow remote attackers to inject arbitrary web script or HTML via (1) a certain referrer field in usercp2.php, (2) a certain location field in inc/functions_online.php, and certain (3) tsubject and (4) psubject fields in moderation.php.	2008-09-10	4.3	CVE-2008-3966
opensc-project -- opensc	pkcs15-tool in OpenSC before 0.11.6 does not apply security updates to a smart card unless the card's label matches the "OpenSC" string, which might allow physically proximate attackers to exploit vulnerabilities that the card owner expected were patched, as demonstrated by exploitation of CVE-2008-2235.	2008-09-10	6.6	CVE-2008-3972
pam_mount -- pam_mount	pam_mount 0.10 through 0.45, when luserconf is enabled, does not verify mountpoint and source ownership before mounting a user-defined volume, which allows local users to bypass intended access restrictions via a local mount.	2008-09-10	6.9	CVE-2008-3970
punbb -- punbb	Cross-site scripting (XSS) vulnerability in userlist.php in PunBB before 1.2.20 allows remote attackers to inject arbitrary web script or HTML via the p parameter.	2008-09-10	4.3	CVE-2008-3968
softalk_mail_server -- softalk_mail_server	The IMAP server in Softalk Mail Server (formerly WorkgroupMail) 8.5.1.431 allows remote authenticated users to cause a denial of service (resource consumption and daemon crash) via a long IMAP	2008-09-11	4.0	CVE-2008-4041

	APPEND command with certain repeated parameters.			
ssmtp -- ssmtp	The from_format function in ssmtp.c in ssmtp 2.62, in certain configurations, uses uninitialized memory for the From: field of an e-mail message, which might allow remote attackers to obtain sensitive information (memory contents) in opportunistic circumstances by reading a message.	2008-09-10	5.0	CVE-2008-3962

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
apple -- quicktime ligos -- invdeo_v5_codec	An unspecified third-party Indeo v5 codec for QuickTime, when used with Apple QuickTime before 7.5.5 on Windows, accesses uninitialized memory, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted movie file.	2008-09-10	0.0	CVE-2008-3615 BID CONFIRM
apple -- itunes	Apple iTunes before 8.0 on Mac OS X 10.4.11, when iTunes Music Sharing is enabled but blocked by the host-based firewall, presents misleading information about firewall security, which might allow remote attackers to leverage an exposure that would be absent if the administrator were given better information.	2008-09-10	2.6	CVE-2008-3634 BID
hp -- hpsi_acf2_connector hp -- hpsi_active_directory_connector hp -- hpsi_bidir_dirx_connector hp -- hpsi_edirectory_connector hp -- hpsi_etrust_connector hp -- hpsi_oid_connector hp -- hpsi_openldap_connector hp -- hpsi_racf_connector hp -- hpsi_sunone_connector hp -- hpsi_topsecret_connector hp -- ibm_tivoli_dir_connector	Unspecified vulnerability in HP OpenView Select Identity (HPSI) Connectors on Windows, as used in HPSI Active Directory Connector 2.30 and earlier, HPSI SunOne Connector 1.14 and earlier, HPSI eDirectory Connector 1.12 and earlier, HPSI eTrust Connector 1.02 and earlier, HPSI OID Connector 1.02 and earlier, HPSI IBM Tivoli Dir Connector 1.02 and earlier, HPSI	2008-09-10	2.1	CVE-2008-3539 HP HP

	TOPSecret Connector 2.22.001 and earlier, HPSI RACF Connector 1.12.001 and earlier, HPSI ACF2 Connector 1.02 and earlier, HPSI OpenLDAP Connector 1.02 and earlier, and HPSI BiDir DirX Connector 1.00.003 and earlier, allows local users to obtain sensitive information via unknown vectors.			
postfix -- postfix linux -- kernel	Postfix 2.4 before 2.4.9, 2.5 before 2.5.5, and 2.6 before 2.6-20080902, when used with the Linux 2.6 kernel, leaks epoll file descriptors during execution of "non-Postfix" commands, which allows local users to cause a denial of service (application slowdown or exit) via a crafted command, as demonstrated by a command in a .forward file.	2008-09-12	2.1	CVE-2008-3889 CONFIRM
postfix -- postfix	Postfix 2.4 before 2.4.9, 2.5 before 2.5.5, and 2.6 before 2.6-20080902, when used with the Linux 2.6 kernel, leaks epoll file descriptors during execution of "non-Postfix" commands, which allows local users to cause a denial of service (application slowdown or exit) via a crafted command, as demonstrated by a command in a .forward file.	2008-09-11	2.1	CVE-2008-4042 CONFIRM

Back to top