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	Published	CVSS Score	Source & Patch Info
airvae -- commerce	SQL injection vulnerability in index.php in Airvae Commerce 3.0 allows remote attackers to execute arbitrary SQL commands via the pid parameter.	2008-11-25	7.5	CVE-2008-5223 XF MILW0RM SECUNIA
apple -- iphone_os	ImageIO in Apple iPhone OS 1.0 through 2.1 and iPhone OS for iPod touch 1.1 through 2.1 allow remote attackers to cause a denial of service (memory consumption and device reset) via a crafted TIFF image.	2008-11-25	7.1	CVE-2008-1586 BID CONFIRM APPLE
apple -- iphone_os	Apple iPhone OS 1.0 through 2.1 and iPhone OS for iPod touch 1.1 through 2.1 changes the encryption level of PPTP VPN connections to a lower level that was previously used, which makes it easier for remote attackers to obtain sensitive information or hijack a connection by decrypting network traffic.	2008-11-25	7.5	CVE-2008-4227 BID CONFIRM APPLE
apple -- safari apple -- iphone_os	Safari in Apple iPhone OS 1.0 through 2.1 and iPhone OS for iPod touch 1.1 through 2.1 does not properly handle HTML TABLE elements, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted HTML document.	2008-11-25	9.3	CVE-2008-4231 BID CONFIRM APPLE
calendarix -- basic	Multiple SQL injection vulnerabilities in Calendarix Basic 0.8.20071118 allow remote attackers to execute arbitrary SQL commands via (1) the catsearch parameter to cal_search.php or (2) the catview parameter to cal_cat.php. NOTE:	2008-11-25	7.5	CVE-2008-2429 MISC SECUNIA

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	vector 1 might overlap CVE-2007-3183.3, and vector 2 might overlap CVE-2005-1865.2.			
debian -- hf	Untrusted search path vulnerability in hfkernel in hf 0.7.3 and 0.8 allows local users to gain privileges via a Trojan horse killall program in a directory in the PATH, related to improper handling of the -k option.	2008-11-26	7.2	CVE-2008-2378 BID DEBIAN SECUNIA
dvbbs -- dvbbs	SQL injection vulnerability in login.asp in Dvbbs 8.2.0 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2008-11-25	7.5	CVE-2008-5222 XF BID BUGTRAQ SECUNIA
mambads -- mambads mambo -- mambo	SQL injection vulnerability in the MambAds (com_mambads) component 1.0 RC1 Beta and 1.0 RC1 for Mambo allows remote attackers to execute arbitrary SQL commands via the ma_cat parameter in a view action to index.php, a different vector than CVE-2007-5177.	2008-11-25	7.5	CVE-2008-5226 BID MILW0RM
microsoft -- windows	Buffer overflow in the CallHTMLHelp method in the Microsoft Windows Media Services ActiveX control in nskey.dll 4.1.00.3917 in Windows Media Services on Microsoft Windows NT and 2000, and Avaya Media and Message Application servers, allows remote attackers to execute arbitrary code via a long argument. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-11-25	9.3	CVE-2008-5232 MISC BID
novell -- iprint	Multiple buffer overflows in Novell iPrint Client before 5.06 allow remote attackers to execute arbitrary code by calling the Novell iPrint ActiveX control (aka ienipp.ocx) with (1) a long third argument to the GetDriverFile method; a long first argument to the (2) GetPrinterURLList or (3) GetPrinterURLList2 method; (4) a long argument to the GetFileList method; a long argument to the (5) GetServerVersion, (6) GetResourceList, or (7) DeleteResource method, related to nipplib.dll; a long uploadPath argument to the (8) UploadPrinterDriver or (9) UploadResource method, related to URIs; (10) a long seventh argument to the UploadResource method; a long string in the (11) second, (12) third, or (13) fourth argument to the GetDriverSettings method, related to the IppGetDriverSettings function in nipplib.dll; or (14) a long eighth argument to the UploadResourceToRMS method.	2008-11-25	9.3	CVE-2008-2431 XF BID MISC SECUNIA

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
novell -- iprint	Stack-based buffer overflow in the ExecuteRequest method in the Novell iPrint ActiveX control in ienipp.ocx in Novell iPrint Client 5.06 and earlier allows remote attackers to execute arbitrary code via a long target-frame option value, a different vulnerability than CVE-2008-2431.	2008-11-25	9.3	CVE-2008-5231 BID MISC SECUNIA
novell -- opensuse novell -- suse_linux novell -- suse_linux_enterprise_server opensuse -- opensuse	yast2-backup 2.14.2 through 2.16.6 on SUSE Linux and Novell Linux allows local users to gain privileges via shell metacharacters in filenames used by the backup process.	2008-11-26	7.2	CVE-2008-4636 BID SUSE
phpcow -- phpcow	Unspecified vulnerability in PHPCow allows remote attackers to execute arbitrary code via unknown vectors, related to a "file inclusion vulnerability," as exploited in the wild in November 2008.	2008-11-25	10.0	CVE-2008-5227 CERT-VN XF BID
redhat -- enterprise_linux redhat -- enterprise_linux_desktop	A certain Red Hat patch for tog-pegasus in OpenGroup Pegasus 2.7.0 does not properly configure the PAM tty name, which allows remote authenticated users to bypass intended access restrictions and send requests to OpenPegasus WBEM services.	2008-11-26	8.5	CVE-2008-4313 CONFIRM
redhat -- enterprise_linux redhat -- enterprise_linux_desktop	tog-pegasus in OpenGroup Pegasus 2.7.0 on Red Hat Enterprise Linux (RHEL) 5, Fedora 9, and Fedora 10 does not log failed authentication attempts to the OpenPegasus CIM server, which makes it easier for remote attackers to avoid detection of password guessing attacks.	2008-11-26	9.3	CVE-2008-4315 CONFIRM CONFIRM CONFIRM XF REDHAT SECUNIA
streamripper -- streamripper	Multiple buffer overflows in lib/http.c in Streamripper 1.63.5 allow remote attackers to execute arbitrary code via (1) a long "Zwitterion v" HTTP header, related to the http_parse_sc_header function; (2) a crafted pls playlist with a long entry, related to the http_get_pls function; or (3) a crafted m3u playlist with a long File entry, related to the http_get_m3u function.	2008-11-25	9.3	CVE-2008-4829 BID BUGTRAQ OSVDB FRSIRT MISC SECUNIA
videoscript -- videoscript	The password change feature (admin/cp.php) in VideoScript 4.0.1.50 and earlier does not check for administrative authentication and does not require knowledge of the original password, which allows remote attackers to change the admin account password via modified npass and npass1 parameters.	2008-11-25	7.5	CVE-2008-5219 MILW0RM SECUNIA OSVDB
wportfolio -- wportfolio	Unrestricted file upload vulnerability in admin/upload_form.php in wPortfolio 0.3 and earlier allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to	2008-11-25	10.0	CVE-2008-5220 XF BID MILW0RM FRSIRT

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	the file in admin/tmp/.			
wportfolio -- wportfolio	The account_save action in admin/userinfo.php in wPortfolio 0.3 and earlier does not require authentication and does not require knowledge of the original password, which allows remote attackers to change the admin account password via modified password and password_retype parameters.	2008-11-25	7.5	CVE-2008-5221 BID MILW0RM FRSIRT
xine -- xine-lib	Multiple heap-based buffer overflows in xine-lib 1.1.12, and other versions before 1.1.15, allow remote attackers to execute arbitrary code via vectors related to (1) a crafted metadata atom size processed by the parse_moov_atom function in demux_qt.c and (2) frame reading in the id3v23_interp_frame function in id3.c. NOTE: as of 20081122, it is possible that vector 1 has not been fixed in 1.1.15.	2008-11-25	9.3	CVE-2008-5234 FRSIRT CONFIRM
xine -- xine	Heap-based buffer overflow in the demux_real_send_chunk function in src/demuxers/demux_real.c in xine-lib before 1.1.15 allows remote attackers to execute arbitrary code via a crafted Real Media file. NOTE: some of these details are obtained from third party information.	2008-11-25	9.3	CVE-2008-5235 FRSIRT CONFIRM SECTRACK SECUNIA
xine -- xine	Multiple heap-based buffer overflows in xine-lib 1.1.12, and other 1.1.15 and earlier versions, allow remote attackers to execute arbitrary code via vectors related to (1) a crafted EBML element length processed by the parse_block_group function in demux_matroska.c; (2) a certain combination of sps, w, and h values processed by the real_parse_audio_specific_data and demux_real_send_chunk functions in demux_real.c; and (3) an unspecified combination of three values processed by the open_ra_file function in demux_realaudio.c. NOTE: vector 2 reportedly exists because of an incomplete fix in 1.1.15.	2008-11-25	9.3	CVE-2008-5236 BID BUGTRAQ MISC FRSIRT FRSIRT MISC SECUNIA SECUNIA
xine -- xine	Multiple integer overflows in xine-lib 1.1.12, and other 1.1.15 and earlier versions, allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via (1) crafted width and height values that are not validated by the mymng_process_header function in demux_mng.c before use in an allocation calculation or (2) crafted current_atom_size and string_size values processed by the parse_reference_atom function in demux_qt.c.	2008-11-25	10.0	CVE-2008-5237 BID BUGTRAQ MISC

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
xine -- xine	Integer overflow in the real_parse_mdpr function in demux_real.c in xine-lib 1.1.12, and other versions before 1.1.15, allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted stream_name_size field.	2008-11-25	7.1	CVE-2008-5238 BID BUGTRAQ MISC CONFIRM SECTRACK
xine -- xine-lib	Unspecified vulnerability in xine-lib before 1.1.15 has unknown impact and attack vectors related to libfaad. NOTE: due to the lack of details, it is not clear whether this is an issue in xine-lib or in libfaad.	2008-11-25	10.0	CVE-2008-5244 CONFIRM SECTRACK
xine -- xine-lib	xine-lib before 1.1.15 performs V4L video frame preallocation before ascertaining the required length, which has unknown impact and attack vectors, possibly related to a buffer overflow in the open_video_capture_device function in src/input/input_v4l.c.	2008-11-25	10.0	CVE-2008-5245 FRSIRT CONFIRM SECTRACK SECUNIA
xine -- xine-lib	Multiple heap-based buffer overflows in xine-lib before 1.1.15 allow remote attackers to execute arbitrary code via vectors that send ID3 data to the (1) id3v22_interp_frame and (2) id3v24_interp_frame functions in src/demuxers/id3.c. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-11-25	9.3	CVE-2008-5246 FRSIRT CONFIRM SECTRACK
xmlsoft -- libxml	Integer overflow in the xmlBufferResize function in libxml2 2.7.2 allows context-dependent attackers to cause a denial of service (infinite loop) via a large XML document.	2008-11-25	7.8	CVE-2008-4225 CONFIRM CONFIRM BID DEBIAN SECUNIA
xmlsoft -- libxml	Integer overflow in the xmlSAX2Characters function in libxml2 2.7.2 allows context-dependent attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a large XML document.	2008-11-25	10.0	CVE-2008-4226 CONFIRM CONFIRM DEBIAN

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
adobe -- flash_media_server	The default configuration of Adobe Flash Media Server (FMS) 3.0 does not enable SWF Verification for (1) RTMPE and (2) RTMPTE sessions, which makes it easier for remote attackers to make copies of video content via stream-capture software.	2008-11-25	5.0	CVE-2008-5109 OSVDB CONFIRM SECUNIA

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
cisco -- cisco	The Temporal Key Integrity Protocol (TKIP) implementation in unspecified Cisco products and other vendors' products, as used in WPA and WPA2 on Wi-Fi networks, has insufficient countermeasures against certain crafted and replayed packets, which makes it easier for remote attackers to decrypt packets from an access point (AP) to a client and spoof packets from an AP to a client, and conduct ARP poisoning attacks or other attacks, as demonstrated by tkiptun-ng.	2008-11-25	6.8	CVE-2008-5230 BID CISCO MISC MISC MISC MLIST MISC MISC
freebsd -- freebsd	The arc4random function in the kernel in FreeBSD 6.3 through 7.1 does not have a proper entropy source for a short time period immediately after boot, which makes it easier for attackers to predict the function's return values and conduct certain attacks against the GEOM framework and various network protocols, related to the Yarrow random number generator.	2008-11-26	6.9	CVE-2008-5162 BID SECTRACK FREEBSD
ibm -- tivoli_access_manager_for_e-business	webseald in WebSEAL 6.0.0.17 in IBM Tivoli Access Manager for e-business allows remote attackers to cause a denial of service (crash or hang) via HTTP requests, as demonstrated by a McAfee vulnerability scan.	2008-11-26	5.0	CVE-2008-5257 BID AIXAPAR
kent-web -- kent-web_mart	Cross-site scripting (XSS) vulnerability in Kent Web Mart 1.61 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-11-25	4.3	CVE-2008-5224 CONFIRM SECUNIA JVN
microsoft -- windows microsoft -- windowst	Stack-based buffer overflow in Microsoft Device IO Control in iphlpapi.dll in Microsoft Windows Vista Gold and SP1 allows local users in the Network Configuration Operator group to gain privileges or cause a denial of service (system crash) via a large invalid PrefixLength to the CreateIpForwardEntry2 method, as demonstrated by a "route add" command.	2008-11-25	6.9	CVE-2008-5229 XF BID BUGTRAQ SECTRACK
novell -- iprint	Insecure method vulnerability in the GetFileList method in an unspecified ActiveX control in Novell iPrint Client before 5.06 allows remote attackers to list the image files in an arbitrary directory via a directory name in the argument.	2008-11-25	5.0	CVE-2008-2432 BID MISC SECUNIA

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
scriptsez -- freeze_greetings	ScriptsEz FREEze Greetings 1.0 stores pwd.txt under the web root with insufficient access control, which allows remote attackers to obtain cleartext passwords.	2008-11-25	5.0	CVE-2008-5218 MILW0RM SECUNIA OSVDB
virtualox -- virtualox	The AcquireDaemonLock function in ipcdUnix.cpp in Sun Innotek VirtualBox before 2.0.6 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/.vbox-$USER-ipc/lock temporary file.	2008-11-26	4.4	CVE-2008-5256 CONFIRM BID
xerox -- docushare	Multiple cross-site scripting (XSS) vulnerabilities in Xerox DocuShare 6 and earlier allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to the default URI under (1) SearchResults/ and (2) Services/ in dsdn/dsweb/, and (3) the default URI under unspecified docushare/dsweb/ServicesLib/Group-#/ directories.	2008-11-25	4.3	CVE-2008-5225 MISC BID BUGTRAQ FRSIRT SECUNIA
xine -- xine-lib	xine-lib 1.1.12, and other versions before 1.1.15, does not check for failure of malloc in circumstances including (1) the mymng_process_header function in demux_mng.c, (2) the open_mod_file function in demux_mod.c, and (3) frame_buffer allocation in the real_parse_audio_specific_data function in demux_real.c, which allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted media file.	2008-11-25	4.3	CVE-2008-5233 BUGTRAQ
xine -- xine-lib	xine-lib 1.1.12, and other 1.1.15 and earlier versions, does not properly handle (a) negative and (b) zero values during unspecified read function calls in input_file.c, input_net.c, input_smb.c, and input_http.c, which allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via vectors such as (1) a file or (2) an HTTP response, which triggers consequences such as out-of-bounds reads and heap-based buffer overflows.	2008-11-25	4.3	CVE-2008-5239 BID
xine -- xine-lib	xine-lib 1.1.12, and other 1.1.15 and earlier versions, relies on an untrusted input value to determine the memory allocation and does not check the result for	2008-11-25	4.3	CVE-2008-5240 BID

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	(1) the MATROSKA_ID_TR_CODECPRIVATE track entry element processed by demux_matroska.c; and (2) PROP_TAG, (3) MDPR_TAG, and (4) CONT_TAG chunks processed by the real_parse_headers function in demux_real.c; which allows remote attackers to cause a denial of service (NULL pointer dereference and crash) or possibly execute arbitrary code via a crafted value.			
xine -- xine-lib	Integer underflow in demux_qt.c in xine-lib 1.1.12, and other 1.1.15 and earlier versions, allows remote attackers to cause a denial of service (crash) via a crafted media file that results in a small value of moov_atom_size in a compressed MOV (aka CMOV_ATOM).	2008-11-25	4.3	CVE-2008-5241 BID
xine -- xine-lib	demux_qt.c in xine-lib 1.1.12, and other 1.1.15 and earlier versions, does not validate the count field before calling calloc for STSD_ATOM atom allocation, which allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted media file.	2008-11-25	6.8	CVE-2008-5242 BID
xine -- xine-lib	The real_parse_headers function in demux_real.c in xine-lib 1.1.12, and other 1.1.15 and earlier versions, relies on an untrusted input length value to "reindex into an allocated buffer," which allows remote attackers to cause a denial of service (crash) via a crafted value, probably an array index error.	2008-11-25	4.3	CVE-2008-5243 BID BUGTRAQ MISC
xine -- xine-lib	The real_parse_audio_specific_data function in demux_real.c in xine-lib 1.1.12, and other 1.1.15 and earlier versions, uses an untrusted height (aka codec_data_length) value as a divisor, which allow remote attackers to cause a denial of service (divide-by-zero error and crash) via a zero value.	2008-11-25	4.3	CVE-2008-5247 BID BUGTRAQ MISC
xine -- xine-lib	xine-lib before 1.1.15 allows remote attackers to cause a denial of service (crash) via "MP3 files with metadata consisting only of separators."	2008-11-25	4.3	CVE-2008-5248 CONFIRM

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**

apple -- iphone_os	The Passcode Lock feature in Apple iPhone OS 1.0 through 2.1 and iPhone OS for iPod touch 1.1 through 2.1 allows physically proximate attackers to leverage the emergency-call ability of locked devices to make a phone call to an arbitrary number.	2008-11-25	3.6	CVE-2008-4228 BID CONFIRM APPLE
apple -- iphone_os	Race condition in the Passcode Lock feature in Apple iPhone OS 2.0 through 2.1 and iPhone OS for iPod touch 2.0 through 2.1 allows physically proximate attackers to remove the lock and launch arbitrary applications by restoring the device from a backup.	2008-11-25	3.7	CVE-2008-4229 BID CONFIRM APPLE
apple -- iphone_os	The Passcode Lock feature in Apple iPhone OS 1.0 through 2.1 and iPhone OS for iPod touch 1.1 through 2.1 displays SMS messages when the emergency-call screen is visible, which allows physically proximate attackers to obtain sensitive information by reading these messages. NOTE: this might be a duplicate of CVE-2008-4593.	2008-11-25	1.9	CVE-2008-4230 BID CONFIRM APPLE
apple -- safari apple -- iphone_os	Safari in Apple iPhone OS 1.0 through 2.1 and iPhone OS for iPod touch 1.1 through 2.1 does not isolate the call-approval dialog from the process of launching new applications, which allows remote attackers to make arbitrary phone calls via a crafted HTML document.	2008-11-25	2.6	CVE-2008-4233 BID CONFIRM SECTRACK APPLE
ibm -- workplace_content_management	Cross-site scripting (XSS) vulnerability in IBM Workplace Content Management (WCM) 6.0G and 6.1 before CF8, when a Page Navigation Component shows menu entries, allows remote attackers to inject arbitrary web script or HTML via unspecified parameters in the URI, related to parameters "not being encoded."	2008-11-25	2.6	CVE-2008-5228 AIXAPAR

Back to top