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**
aspindir -- iltaweb_alisveris_sistemi	SQL injection vulnerability in urunler.asp in Iltaweb Alisveris Sistemi allows remote attackers to execute arbitrary SQL commands via the catno parameter.	2008-12-24	7.5	CVE-2008-5707 BID BUGTRAQ
avaya -- communication_manager	Multiple unspecified vulnerabilities in the web management interface in Avaya Communication Manager (CM) 3.1 before 3.1.4 SP2, 4.0 before 4.0.3 SP1, and 5.0 before 5.0 SP3 allow remote authenticated users to execute arbitrary code via unknown attack vectors in the (1) Set Static Routes and (2) Backup	2008-12-24	9.0	CVE-2008-5709 XF XF MISC MISC BID FRSIRT CONFIRM SECUNIA
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	History components.			
facebook -- photouploader	Heap-based buffer overflow in the Facebook PhotoUploader ActiveX control 5.0.14.0 and earlier allows remote attackers to execute arbitrary code via a long FileMask property value.	2008-12-24	9.3	CVE-2008-5711 MILW0RM
libvirt -- libvirt	xend in Xen 3.3.0 does not properly restrict a guest VM's write access within the /local/domain xenstore directory tree, which allows guest OS users to cause a denial of service and possibly have unspecified other impact by writing to (1) console/tty, (2) console/limit, or (3) image/device-model-pid. NOTE: this issue exists because of erroneous set_permissions calls in the fix for CVE-2008-4405.	2008-12-24	7.2	CVE-2008-5716 MLIST MLIST MLIST MLIST MLIST
novell -- netware	Novell NetWare 6.5 before Support Pack 8, when an OES2 Linux server is installed into the NDS tree, does not require a password for the ApacheAdmin console, which allows remote attackers to reconfigure the Apache HTTP Server via console operations.	2008-12-19	9.3	CVE-2008-5696 SECTRACK BID CONFIRM FRSIRT SECUNIA
php -- php	Heap-based buffer overflow in ext/mbstring/libmbfl/filters /mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2)	2008-12-23	10.0	CVE-2008-5557 XF BID CONFIRM SECTRACK CONFIRM CONFIRM FULLDISC

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.			
php-collab -- php-collab	Static code injection vulnerability in installation/setup.php in phpCollab 2.5 rc3 and earlier allows remote authenticated administrators to inject arbitrary PHP code into include/settings.php via the URI.	2008-12-23	9.0	CVE-2008-4305 XF BID GENTOO SECUNIA SECUNIA CONFIRM
phpcollab -- phpcollab	general/login.php in phpCollab 2.5 rc3 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in unspecified input related to the SSL_CLIENT_CERT environment variable. NOTE: in some environments, SSL_CLIENT_CERT always has a base64-encoded string value, which may impose constraints on injection for typical shells.	2008-12-23	10.0	CVE-2008-4304 XF BID GENTOO SECUNIA CONFIRM
qemu -- qemu	Off-by-one error in monitor.c in Qemu 0.9.1 might make it easier for remote attackers to guess the VNC password, which is limited to seven characters where eight was intended.	2008-12-24	7.8	CVE-2008-5714 CONFIRM CONFIRM MLIST MLIST
slimcms -- slimcms	redirect.php in SlimCMS 1.0.0 does not require authentication, which allows remote attackers to create administrative users by using the newusername and newpassword parameters and setting the newisadmin parameter to 1.	2008-12-24	7.5	CVE-2008-5708 XF BID MILW0RM
trend_micro -- housecall	The Trend Micro HouseCall ActiveX control 6.51.0.1028 and 6.6.0.1278 in	2008-12-23	9.3	CVE-2008-2434 XF BID
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	Housecall_ActiveX.dll allows remote attackers to download an arbitrary library file onto a client system via a "custom update server" argument. NOTE: this can be leveraged for code execution by writing to a Startup folder.			BUGTRAQ MISC SECUNIA MISC
trend_micro -- housecall	Use-after-free vulnerability in the Trend Micro HouseCall ActiveX control 6.51.0.1028 and 6.6.0.1278 in Housecall_ActiveX.dll allows remote attackers to execute arbitrary code via a crafted notifyOnLoadNative callback function.	2008-12-23	9.3	CVE-2008-2435 XF BID BUGTRAQ OSVDB SECTRACK MISC SECUNIA CONFIRM
Back to top				

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
avaya -- communication_manager	Multiple unspecified vulnerabilities in the web management interface in Avaya Communication Manager (CM) 3.1.x, 4.0.3, and 5.x allow remote attackers to read (1) configuration files, (2) log files, (3) binary image files, and (4) help files via unknown vectors.	2008-12-24	5.0	CVE-2008-5710 XF MISC BID FRSIRT CONFIRM SECUNIA
konqueror -- konqueror	The HTML parser in KDE Konqueror 3.5.9 allows remote attackers to cause a denial of service (application crash) via (1) a long COLOR attribute in an HR element; or a long (a) BGCOLOR or (b) BORDERCOLOR attribute in a (2) TABLE, (3) TD, or (4) TR element. NOTE: the FONT vector is already covered by	2008-12-24	5.0	CVE-2008-5712 MILW0RM
Back to top				

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	CVE-2008-4514.			
kvm_qumranet -- kvm qemu -- qemu	The protocol_client_msg function in vnc.c in the VNC server in (1) Qemu 0.9.1 and earlier and (2) KVM kvm-79 and earlier allows remote attackers to cause a denial of service (infinite loop) via a certain message.	2008-12-24	5.0	CVE-2008-2382 BID BUGTRAQ FRSIRT FRSIRT MISC SECTRACK SECTRACK SECUNIA SECUNIA
linux -- kernel	The __qdisc_run function in net/sched/sch_generic.c in the Linux kernel before 2.6.25 on SMP machines allows local users to cause a denial of service (soft lockup) by sending a large amount of network traffic, as demonstrated by multiple simultaneous invocations of the Netperf benchmark application in UDP_STREAM mode.	2008-12-24	4.9	CVE-2008-5713 CONFIRM BID MLIST CONFIRM CONFIRM
mozilla -- firefox	Mozilla Firefox 3.0.5 on Windows Vista allows remote attackers to cause a denial of service (application crash) via JavaScript code with a long string value for the hash property (aka location.hash).	2008-12-24	5.0	CVE-2008-5715 BID MILW0RM
php-collab -- php-collab	Multiple SQL injection vulnerabilities in phpCollab 2.5 rc3, 2.4, and earlier allow remote attackers to execute arbitrary SQL commands via the loginForm parameter to general/login.php, and unspecified other vectors.	2008-12-23	6.8	CVE-2008-4303 XF BID GENTOO SECUNIA SECUNIA CONFIRM
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the X Inter Client Exchange library (aka	2008-12-19	5.0	CVE-2008-5684 SUNALERT

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	libICE) in Sun Solaris 8 through 10 and OpenSolaris before snv_85 allows context-dependent attackers to cause a denial of service (application crash), as demonstrated by a port scan that triggers a segmentation violation in the Gnome session manager (aka gnome-session).			CONFIRM
university_of_washington -- imap	Off-by-one error in the rfc822_output_char function in the RFC822BUFFER routines in the University of Washington (UW) c-client library, as used by the UW IMAP toolkit before imap-2007e and other applications, allows context-dependent attackers to cause a denial of service (crash) via an e-mail message that triggers a buffer overflow.	2008-12-23	4.3	CVE-2008-5514 CONFIRM XF CONFIRM SECTRACK SECUNIA
Back to top				

There were no low vulnerabilities recorded this week.