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
Adobe -- Acrobat Standard Adobe -- Acrobat Professional Adobe -- Acrobat 3D Adobe -- Acrobat Reader	The Javascript API in Adobe Acrobat Professional 7.0.9 and possibly 8.1.1 exposes a dangerous method, which allows remote attackers to (1) execute arbitrary commands or (2) trigger a buffer overflow via a crafted PDF file that invokes app.checkForUpdate with a malicious callback function.	unknown 2008-05-07	9.3	CVE-2008-2042 BUGTRAQ OTHER-REF SECTRACK XF
backlinkspider -- backlink_spider	SQL injection vulnerability in BackLinkSpider allows remote attackers to execute arbitrary SQL commands via the cat_id parameter to a site-specific component name such as link.php or backlinkspider.php.	unknown 2008-05-07	7.5	CVE-2008-2096 BUGTRAQ MILW0RM BID XF
CMS Faethon -- CMS Faethon	Cross-site scripting (XSS) vulnerability in search.php in CMS Faethon 2.2 Ultimate allows remote attackers to inject arbitrary web script or HTML via the what parameter. NOTE: some of these details are obtained from third party information.	unknown 2008-05-09	7.5	CVE-2008-2127 MILW0RM BID

fipsASP -- fipsCMS	SQL injection vulnerability in modules/print.asp in fipsASP fipsCMS allows remote attackers to execute arbitrary SQL commands via the lg parameter.	unknown 2008-05-09	7.5	CVE-2008-2124 MILW0RM BID
HP -- LDAP-UX	Unspecified vulnerability in HP LDAP-UX vB.04.10 through vB.04.15 allows local users to gain privileges via unknown vectors.	unknown 2008-05-07	7.2	CVE-2008-1659 BID
kubelabs -- kubelance	Directory traversal vulnerability in ipn.php in KubeLabs Kubelance 1.6.4 allows remote attackers to include and execute arbitrary local files via the i parameter.	unknown 2008-05-06	7.5	CVE-2008-2091 MILW0RM BID XF
Linksys -- SPA-2102 Phone Adapter	Linksys SPA-2102 Phone Adapter 3.3.6 allows remote attackers to cause a denial of service (crash) via a long ping packet ("ping of death"). NOTE: the severity of this issue has been disputed since there are limited attack scenarios.	unknown 2008-05-06	7.8	CVE-2008-2092 BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BID XF
Mambo -- com_comprofiler Joomla -- com_comprofiler JoomlaPolis -- community_builder	SQL injection vulnerability in the Profiler (com_comprofiler) component in Community Builder for Mambo and Joomla! allows remote attackers to execute arbitrary SQL commands via the user parameter in a userProfile action to index.php.	unknown 2008-05-06	7.5	CVE-2008-2093 MILW0RM BID
Mambo -- com_flippingbook Joomla -- com_flippingbook page-flip-tools -- flipping_book	SQL injection vulnerability in index.php in the FlippingBook (com_flippingbook) 1.0.4 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the book_id parameter.	unknown 2008-05-06	7.5	CVE-2008-2095 MILW0RM BID XF
MusicBox -- MusicBox	SQL injection vulnerability in viewalbums.php in Musicbox 2.3.6 and 2.3.7 allows remote attackers to execute arbitrary SQL commands via the artistId parameter.	unknown 2008-05-09	7.5	CVE-2008-2125 MILW0RM BID
MyArticles -- MyArticles RunCMS -- myarticles_module	SQL injection vulnerability in topics.php in the MyArticles 0.6 beta-1 module for RunCMS allows remote attackers to execute arbitrary SQL commands via the topic_id parameter in a listarticles action.	unknown 2008-05-05	7.5	CVE-2008-2084 MILW0RM BID XF
NASA Goddard Space Flight Center -- Common Data Format	Stack-based buffer overflow in the Read32s_64 function in src/lib/cdfread64.c in the NASA Goddard Space Flight Center Common Data Format (CDF) library before 3.2.1 allows context-dependent attackers to execute arbitrary code via a .cdf file with	unknown 2008-05-06	7.5	CVE-2008-2080 OTHER-REF BID

	crafted length tags.			
PHP -- PHP	cgi_main.c in PHP before 5.2.6 does not properly calculate the length of PATH_TRANSLATED, which has unknown impact and attack vectors.	unknown 2008-05-05	10.0	CVE-2008-0599 OTHER-REF OTHER-REF
PHP -- PHP	Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors	unknown 2008-05-05	10.0	CVE-2008-2050 OTHER-REF OTHER-REF
PHP -- PHP	The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."	unknown 2008-05-05	10.0	CVE-2008-2051 OTHER-REF
PHP -- PHP	The GENERATE_SEED macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 32-bit systems, performs a multiplication using values that can produce a zero seed in rare circumstances, which allows context-dependent attackers to predict subsequent values of the rand and mt_rand functions and possibly bypass protection mechanisms that rely on an unknown initial seed.	unknown 2008-05-07	7.5	CVE-2008-2107 BUGTRAQ FULLDISC OTHER-REF XF
PHP -- PHP	The GENERATE_SEED macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 64-bit systems, performs a multiplication that generates a portion of zero bits during conversion due to insufficient precision, which produces 24 bits of entropy and simplifies brute force attacks against protection mechanisms that use the rand and mt_rand functions.	unknown 2008-05-07	7.5	CVE-2008-2108 BUGTRAQ FULLDISC OTHER-REF XF
phpeasydata -- phpeasydata	SQL injection vulnerability in annuaire.php in PHPEasyData 1.5.4 allows remote attackers to execute arbitrary SQL commands via the cat_id parameter.	unknown 2008-05-08	7.5	CVE-2008-2113 MILW0RM BID XF
phpforge -- php_forge	SQL injection vulnerability in admin/news.php in PHP Forge 3.0 beta 2 allows remote attackers to execute arbitrary SQL commands via the id parameter in the news module to admin.php.	unknown 2008-05-06	7.5	CVE-2008-2088 MILW0RM BID XF
PreProjects.com -- Pre Shopping Mall	SQL injection vulnerability in emall/search.php in Pre Shopping Mall 1.1 allows remote attackers to execute arbitrary SQL commands via the search parameter.	unknown 2008-05-08	7.5	CVE-2008-2114 MILW0RM BID XF

Project Alumni -- Project Alumni	SQL injection vulnerability in info.php in Project Alumni 1.0.9 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-05-08	7.5	CVE-2008-2118 BUGTRAQ BID XF
QTO -- QTOFileManager	Unrestricted file upload vulnerability in qtofm.php in QTOFileManager 1.0 allows remote attackers to execute arbitrary PHP code by uploading a file with an executable extension, then accessing it via a direct request.	unknown 2008-05-07	7.5	CVE-2008-2110 BUGTRAQ BID XF
redhat -- enterprise_linux redhat -- desktop	The IPsec implementation in Linux kernel before 2.6.25 allows remote routers to cause a denial of service (crash) via a fragmented ESP packet in which the first fragment does not contain the entire ESP header and IV.	unknown 2008-05-07	7.1	CVE-2007-6282 MLIST OTHER-REF REDHAT
Siteman -- Siteman	Directory traversal vulnerability in index.php in Siteman 2.0.x2 allows remote authenticated administrators to include and execute arbitrary local files via a .. (dot dot) in the module parameter.	unknown 2008-05-05	9.0	CVE-2008-2081 MILW0RM OTHER-REF BID XF XF
Sun -- Solaris	Unspecified vulnerability in the SCTP protocol implementation in Sun Solaris 10 allows remote attackers to cause a denial of service (panic) via a crafted SCTP packet.	unknown 2008-05-06	7.8	CVE-2008-2089 SUNALERT XF
Sun -- Solaris	Unspecified vulnerability in the SCTP protocol implementation in Sun Solaris 10 allows remote attackers to cause a denial of service (CPU consumption and network traffic amplification) via a crafted SCTP packet.	unknown 2008-05-06	7.8	CVE-2008-2090 SUNALERT XF
Sun -- Ray Server Software	Unspecified vulnerability in Sun Ray Kiosk Mode 4.0 allows local and remote authenticated Sun Ray administrators to gain root privileges via unknown vectors related to utconfig.	unknown 2008-05-07	9.3	CVE-2008-2112 SUNALERT BID
Sun -- Solaris	The TCP implementation in Sun Solaris 8, 9, and 10 allows remote attackers to cause a denial of service (CPU consumption and new connection timeouts) via a TCP SYN flood attack.	unknown 2008-05-09	7.8	CVE-2008-2121 SUNALERT SECTRACK XF
Systementor -- PostcardMentor	SQL injection vulnerability in step1.asp in Systementor PostcardMentor allows remote attackers to execute arbitrary SQL commands via the cat_fldAuto parameter.	unknown 2008-05-09	7.5	CVE-2008-2132 MILW0RM BID

Tux -- CMS	Multiple cross-site scripting (XSS) vulnerabilities in Tux CMS 0.1 allow remote attackers to inject arbitrary web script or HTML via the (1) q parameter to index.php and the (2) returnURL parameter to tux-login.php.	unknown 2008-05-09	7.5	CVE-2008-2126 BUGTRAQ BID
VisualShapers -- ezContents	Multiple SQL injection vulnerabilities in VisualShapers ezContents 2.0.0 allow remote attackers to execute arbitrary SQL commands via the (1) contentname parameter to showdetails.php and the (2) article parameter to printer.php.	unknown 2008-05-09	7.5	CVE-2008-2135 BUGTRAQ MILW0RM BID
XOOPS -- Article Module	SQL injection vulnerability in article.php in the Article module for XOOPS allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-05-06	7.5	CVE-2008-2094 BUGTRAQ BID XF
Yahoo -- yahoo_assistant	The ActiveX Control (yNotifier.dll) in Yahoo! Assistant 3.6 and earlier allows remote attackers to execute arbitrary code via unspecified vectors in the Ynoifier COM object that trigger memory corruption.	unknown 2008-05-07	9.3	CVE-2008-2111 OTHER-REF BID XF

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Activision -- call_of_duty_4	Call of Duty 4 (CoD4) 1.5 and earlier allows remote authenticated users to cause a denial of service (crash) via a type 7 stats packet, which triggers a memcpy with a negative value.	unknown 2008-05-07	6.8	CVE-2008-2106 BUGTRAQ OTHER-REF BID
Cine -- Galleristic	SQL injection vulnerability in index.php in Galleristic 1.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the cat parameter.	unknown 2008-05-09	6.8	CVE-2008-2129 MILW0RM BID
CMS Faethon -- CMS Faethon	PHP remote file inclusion vulnerability in templates/header.php in CMS Faethon 2.2 Ultimate allows remote attackers to execute arbitrary PHP code via a URL in the mainpath parameter, a different vulnerability than CVE-2006-5588 and CVE-2006-3185.	unknown 2008-05-09	6.8	CVE-2008-2128 MILW0RM
IBM -- Rational Build Forge	IBM Rational Build Forge 7.0.2 allows remote attackers to cause a denial of service (CPU consumption) via a port scan, which spawns multiple bfagent server processes that attempt	unknown 2008-05-09	5.0	CVE-2008-2122 OTHER-REF BID SECTRACK

	to read data from closed sockets.			
iGaming -- CMS	SQL injection vulnerability in poll_vote.php in iGaming CMS 1.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-05-09	6.8	CVE-2008-2130 OTHER-REF BID XF
Linux -- Kernel	The Xen hypervisor block backend driver for Linux kernel 2.6.18, when running on a 64-bit host with a 32-bit paravirtualized guest, allows local privileged users in the guest OS to cause a denial of service (host OS crash) via a request that specifies a large number of blocks.	unknown 2008-05-07	4.9	CVE-2007-5498 REDHAT
Linux -- Kernel	Linux kernel before 2.6.25.2 does not apply a certain protection mechanism for fcntl functionality, which allows local users to (1) execute code in parallel or (2) exploit a race condition to obtain "re-ordered access to the descriptor table."	unknown 2008-05-07	6.9	CVE-2008-1669 OTHER-REF REDHAT REDHAT REDHAT
media-libs -- libid3tag	field.c in the libid3tag 0.15.0b library allows context-dependent attackers to cause a denial of service (CPU consumption) via an ID3_FIELD_TYPE_STRINGLIST field that ends in '\0', which triggers an infinite loop.	unknown 2008-05-07	5.0	CVE-2008-2109 MLIST
Mozilla -- Bugzilla	Cross-site scripting (XSS) vulnerability in Bugzilla 2.17.2 and later allows remote attackers to inject arbitrary web script or HTML via the id parameter to the "Format for Printing" view or "Long Format" bug list.	unknown 2008-05-07	4.3	CVE-2008-2103 OTHER-REF OTHER-REF BID SECTRACK XF
Mozilla -- Bugzilla	The WebService in Bugzilla before 3.1.3 allows remote authenticated users without canconfirm privileges to create NEW or ASSIGNED bug entries via a request to the XML-RPC interface, which bypasses the canconfirm check.	unknown 2008-05-07	4.0	CVE-2008-2104 OTHER-REF OTHER-REF BID SECTRACK XF
MySQL -- MySQL	MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are within the MySQL home data directory, which can point to tables that are created in the future.	unknown 2008-05-05	6.8	CVE-2008-2079 OTHER-REF OTHER-REF OTHER-REF OTHER-REF
MyVietnam -- mvnForum	Cross-site scripting (XSS) vulnerability in mvnForum 1.1 GA allows remote authenticated users to inject arbitrary web	unknown 2008-05-09	4.3	CVE-2008-2131 OTHER-REF BID

	script or HTML via the topic field, which is later displayed by user/viewthread.jsp through use of the "quick reply button."			XF
Project Alumni -- Project Alumni	Cross-site scripting (XSS) vulnerability in pages/news.page.inc in Project Alumni 1.0.9 allows remote attackers to inject arbitrary web script or HTML via the year parameter in a news action to index.php, a different vector than CVE-2007-6126.	unknown 2008-05-08	4.3	CVE-2008-2117 BUGTRAQ BID XF
ProZIlla -- hosting_index	SQL injection vulnerability in directory.php in Prozilla Hosting Index, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a list action.	unknown 2008-05-05	6.8	CVE-2008-2083 BUGTRAQ MILW0RM BID
Red Hat -- Desktop redhat -- enterprise_linux	Linux kernel before 2.4.21 allows local users to cause a denial of service (kernel panic) via asynchronous input or output on a FIFO special file.	unknown 2008-05-07	4.9	CVE-2007-5001 OTHER-REF REDHAT
redhat -- enterprise_linux redhat -- desktop	Linux kernel 2.6.18, and possibly other versions, when running on AMD64 architectures, allows local users to cause a denial of service (crash) via certain ptrace calls.	unknown 2008-05-07	4.9	CVE-2008-1615 OTHER-REF REDHAT
SAP -- Internet Transaction Server	Cross-site scripting (XSS) vulnerability in WGate in SAP Internet Transaction Server (ITS) 6.20 allows remote attackers to inject arbitrary web script or HTML via (1) a "<>" sequence in the ~service parameter to wgate.dll, or (2) Javascript splicing in the query string, a different vector than CVE-2006-5114.	unknown 2008-05-09	4.3	CVE-2008-2123 OTHER-REF BID XF
ScriptsEZ -- Power Editor	Multiple cross-site scripting (XSS) vulnerabilities in editor.php in ScriptsEZ.net Power Editor 2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) te and (2) dir parameters in a tempedit action.	unknown 2008-05-08	4.3	CVE-2008-2115 BUGTRAQ MILW0RM BID XF
ScriptsEZ -- Power Editor	Multiple directory traversal vulnerabilities in editor.php in ScriptsEZ.net Power Editor 2.0 allow remote attackers to read arbitrary local files via a .. (dot dot) in the (1) te and (2) dir parameters in a tempedit action.	unknown 2008-05-08	4.4	CVE-2008-2116 BUGTRAQ MILW0RM BID XF
Siteman -- Siteman	Cross-site scripting (XSS) vulnerability in index.php in Siteman 2.0.x2 allows remote attackers to inject arbitrary web script or HTML via the module parameter, which leaks the path in an error message.	unknown 2008-05-05	4.3	CVE-2008-2082 MILW0RM OTHER-REF BID XF

SoftBiz -- Web Hosting Directory Script	SQL injection vulnerability in search_result.php in Softbiz Web Host Directory Script, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the host_id parameter, a different vector than CVE-2005-3817.	unknown 2008-05-06	6.8	CVE-2008-2087 BUGTRAQ MILW0RM BID
Sun -- Java System Application Server Sun -- Java System Web Server	Unspecified vulnerability in Sun Java System Application Server 7 2004Q2 before Update 6, Web Server 6.1 before SP8, and Web Server 7.0 before Update 1 allows remote attackers to obtain source code of JSP files via unknown vectors.	unknown 2008-05-09	5.0	CVE-2008-2120 SECTRACK SECTRACK
Tru-Zone -- NukeET	Cross-site scripting (XSS) vulnerability in the Journal module in Tru-Zone Nuke ET 3.x allows remote attackers to inject arbitrary web script or HTML via the title parameter in a new entry, as demonstrated by a CSS property in the STYLE attribute of a DIV element, a different vulnerability than CVE-2008-1873.	unknown 2008-05-09	4.3	CVE-2008-2133 OTHER-REF OTHER-REF BID XF
Tru-Zone -- NukeET	The Journal module in Tru-Zone Nuke ET 3.x allows remote attackers to obtain access to arbitrary user accounts, and alter or delete data, via a modified username in an unspecified cookie.	unknown 2008-05-09	5.8	CVE-2008-2134 OTHER-REF XF
Wonderware -- SuiteLink Wonderware -- InTouch	The SuiteLink Service (aka slssvc.exe) in WonderWare SuiteLink before 2.0 Patch 01, as used in WonderWare InTouch 8.0, allows remote attackers to cause a denial of service (NULL pointer dereference and service shutdown) and possibly execute arbitrary code via a large length value in a Registration packet to TCP port 5413, which causes a memory allocation failure.	unknown 2008-05-06	5.0	CVE-2008-2005 BUGTRAQ OTHER-REF BID

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Mozilla -- Bugzilla	email_in.pl in Bugzilla 2.23.4, and later versions before 3.0, allows remote authenticated users to more easily spoof the changer of a bug via a @reporter command in the body of an e-mail message, which overrides the e-mail address as normally	unknown 2008-05-07	3.5	CVE-2008-2105 OTHER-REF OTHER-REF BID SECTRACK

	obtained from the From e-mail header. NOTE: since From headers are easily spoofed, this only crosses privilege boundaries in environments that provide additional verification of e-mail addresses.	

Back to top