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**
2500mhz -- worksimple	PHP remote file inclusion vulnerability in calendar.php in WorkSimple 1.2.1, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the lang parameter.	2008-12-30	9.3	CVE-2008-5764 XF BID MILW0RM SECUNIA OSVDB
alstrasoft -- web_email_script_enterprise	SQL injection vulnerability in index.php in AlstraSoft Web Email Script Enterprise (ESE) allows remote attackers to execute arbitrary SQL commands via the id parameter in a directory action.	2008-12-30	7.5	CVE-2008-5751 BID MILW0RM
apertoblog -- apertoblog	SQL injection vulnerability in categories.php in Aperto Blog 0.1.1 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-30	7.5	CVE-2008-5775 XF BID MILW0RM
apertoblog -- apertoblog	Multiple directory traversal vulnerabilities in Aperto Blog 0.1.1 allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the (1)	2008-12-30	7.5	CVE-2008-5776 BID MILW0RM
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	action parameter to admin.php and the (2) get parameter to index.php. NOTE: in some environments, this can be leveraged for remote file inclusion by using a UNC share pathname or an ftp, ftps, or ssh2.sftp URL.			
aspsiteware -- realtylistings	Multiple SQL injection vulnerabilities in ASPSiteWare RealtyListings 1.0 and 2.0 allow remote attackers to execute arbitrary SQL commands via the (1) iType parameter to type.asp and the (2) iPro parameter to detail.asp.	2008-12-30	7.5	CVE-2008-5772 XF MILW0RM SECUNIA OSVDB OSVDB
aspsiteware -- homebuilder	Multiple SQL injection vulnerabilities in ASPSiteWare HomeBuilder 1.0 and 2.0 allow remote attackers to execute arbitrary SQL commands via the (1) iType parameter to (a) type.asp and (b) type2.asp and the (2) iPro parameter to (c) detail.asp.	2008-12-30	7.5	CVE-2008-5774 XF MILW0RM SECUNIA
bpftp -- bulletproof_ftp_client	Stack-based buffer overflow in BulletProof FTP Client 2.63 allows user-assisted attackers to execute arbitrary code via a bookmark file entry with a long host name.	2008-12-30	9.3	CVE-2008-5753 BID MILW0RM SECUNIA OSVDB
bpftp -- bulletproof_ftp_client	Stack-based buffer overflow in BulletProof FTP Client allows user-assisted attackers to execute arbitrary code via a .bps file (aka Session-File) with a long second line, possibly a related issue to CVE-2008-5753.	2008-12-30	9.3	CVE-2008-5754 BID MILW0RM
cadenix -- cadenix	SQL injection vulnerability in index.php in CadeNix allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2008-12-30	7.5	CVE-2008-5777 XF BID MILW0RM
cfagcms -- cfagcms	SQL injection vulnerability in right.php in Cant Find A Gaming CMS (CFAGCMS) 1.0 Beta 1 allows remote attackers to execute arbitrary SQL commands via the title parameter.	2008-12-30	7.5	CVE-2008-5781 XF MILW0RM
deltascripts -- php_classifieds	SQL injection vulnerability in detail.php in DeltaScripts PHP	2008-12-31	7.5	CVE-2008-5805 XF

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	Classifieds 7.5 and earlier allows remote attackers to execute arbitrary SQL commands via the siteid parameter, a different vector than CVE-2006-5828.			BID MILW0RM FRSIRT
deltascripts -- php_classifieds	SQL injection vulnerability in login.php in DeltaScripts PHP Classifieds 7.5 and earlier allows remote attackers to execute arbitrary SQL commands via the admin_username parameter (aka admin field). NOTE: some of these details are obtained from third party information.	2008-12-31	7.5	CVE-2008-5806 XF BID MILW0RM SECUNIA
domainsellerpro -- domain_seller_pro	SQL injection vulnerability in index.php in Domain Seller Pro 1.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-31	7.5	CVE-2008-5788 BID MILW0RM FRSIRT SECUNIA
e-topbiz -- online_store	SQL injection vulnerability in index.php in E-topbiz Online Store 1.0 allows remote attackers to execute arbitrary SQL commands via the cat_id parameter.	2008-12-31	7.5	CVE-2008-5802 XF MILW0RM FRSIRT SECUNIA
e-topbiz -- online_store	SQL injection vulnerability in admin/login.php in E-topbiz Online Store 1.0 allows remote attackers to execute arbitrary SQL commands via the user parameter (aka username field). NOTE: some of these details are obtained from third party information.	2008-12-31	7.5	CVE-2008-5803 MILW0RM SECUNIA
e-topbiz -- number_links_1_php_script	SQL injection vulnerability in admin/admin_catalog.php in e-topbiz Number Links 1 Php Script allows remote attackers to execute arbitrary SQL commands via the id parameter in an edit action.	2008-12-31	7.5	CVE-2008-5804 BID MILW0RM SECUNIA
fascript -- faupload	SQL injection vulnerability in download.php in Farsi Script Faupload allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-30	7.5	CVE-2008-5766 XF BID MILW0RM
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
flds_script -- flds	SQL injection vulnerability in report.php in Free Links Directory Script (FLDS) 1.2a allows remote attackers to execute arbitrary SQL commands via the linkid parameter.	2008-12-30	7.5	CVE-2008-5778 XF BID MILW0RM SECUNIA OSVDB
flds_script -- flds	SQL injection vulnerability in lpro.php in Free Links Directory Script (FLDS) 1.2a allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-30	7.5	CVE-2008-5779 BID MILW0RM SECUNIA OSVDB
gazatem -- gnews_publisher	SQL injection vulnerability in authors.asp in gNews Publisher allows remote attackers to execute arbitrary SQL commands via the authorID parameter.	2008-12-30	7.5	CVE-2008-5767 BID MILW0RM SECUNIA
invisible-island -- xterm	The default configuration of xterm on Debian GNU/Linux sid and possibly Ubuntu enables the allowWindowOps resource, which allows user-assisted attackers to execute arbitrary code or have unspecified other impact via escape sequences.	2009-01-02	10.0	CVE-2006-7236 CONFIRM CONFIRM
invisible-island -- xterm	CRLF injection vulnerability in xterm allows user-assisted attackers to execute arbitrary commands via LF (aka \n) characters surrounding a command name within a Device Control Request Status String (DECRQSS) escape sequence in a text file, a related issue to CVE-2003-0063 and CVE-2003-0071.	2009-01-02	9.3	CVE-2008-2383 SECUNIA CONFIRM
kvm_qumranet -- kvm qemu -- qemu	Heap-based buffer overflow in the Cirrus VGA implementation in (1) KVM before kvm-82 and (2) QEMU on Debian GNU/Linux and Ubuntu might allow local users to gain privileges by using the VNC console for a connection, aka the LGD-54XX "bitblt" heap overflow. NOTE: this issue exists because of an incorrect fix for CVE-2007-1320.	2008-12-29	7.2	CVE-2008-4539 FEDORA CONFIRM CONFIRM CONFIRM CONFIRM MLIST MLIST SECUNIA SECUNIA SECUNIA

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
				MLIST CONFIRM
mariovaldez -- simple_text-file_login_script	PHP remote file inclusion vulnerability in slogin_lib.inc.php in Simple Text-File Login Script (SiTeFiLo) 1.0.6 allows remote attackers to execute arbitrary PHP code via a URL in the slogin_path parameter.	2008-12-30	7.5	CVE-2008-5763 MILW0RM SECUNIA OSVDB
phpweather -- phpweather	Directory traversal vulnerability in test.php in PHP Weather 2.2.2 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the language parameter.	2008-12-30	7.5	CVE-2008-5771 BID MILW0RM SECUNIA
prestashop -- prestashop	Multiple unspecified vulnerabilities in PrestaShop e-Commerce Solution before 1.1 Beta 2 (aka 1.1.0.1) have unknown impact and attack vectors, related to the (1) bankwire module, (2) cheque module, and other components.	2008-12-31	10.0	CVE-2008-5791 BID
recly -- interactive_feederator	Multiple PHP remote file inclusion vulnerabilities in the Recly Interactive Feederator (com_feederator) component 1.0.5 for Joomla! allow remote attackers to execute arbitrary PHP code via a URL in the (1) mosConfig_absolute_path parameter to (a) add_tmsp.php, (b) edit_tmsp.php and (c) tmsp.php in includes/tmsp/; and the (2) GLOBALS[mosConfig_absolute_path] parameter to (d) includes/tmsp /subscription.php.	2008-12-31	7.5	CVE-2008-5789 XF BID MILW0RM
recly -- competitions	Multiple PHP remote file inclusion vulnerabilities in the Recly!Competitions (com_competitions) component 1.0 for Joomla! allow remote attackers to execute arbitrary PHP code via a URL in the (1) GLOBALS[mosConfig_absolute_path] parameter to (a) add.php and (b) competitions.php in	2008-12-31	7.5	CVE-2008-5790 BID MILW0RM
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	includes/competitions/, and the (2) mosConfig_absolute_path parameter to (c) includes/settings/settings.php.			
sirium -- am_events_module	SQL injection vulnerability in print.php in the AM Events (aka Amevents) module 0.22 for XOOPS allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-30	7.5	CVE-2008-5768 XF BID MILW0RM
typo3 -- eluna_page_comments_extension	SQL injection vulnerability in the eluna Page Comments (eluna_pagecomments) extension 1.1.2 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-12-31	7.5	CVE-2008-5796 BID CONFIRM SECUNIA
typo3 -- advcalendar_extension	SQL injection vulnerability in the advCalendar extension 0.3.1 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-12-31	7.5	CVE-2008-5797 CONFIRM
typo3 -- cms_poll_system_extension	SQL injection vulnerability in the CMS Poll system (cms_poll) extension before 0.1.1 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-12-31	7.5	CVE-2008-5798 CONFIRM
typo3 -- fsmi_people typo3 -- wir_ber_uns_extension	SQL injection vulnerability in the Wir ber uns [sic] (fsmi_people) extension 0.0.24 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-12-31	7.5	CVE-2008-5800 CONFIRM
typo3 -- dictionary_extension	Unspecified vulnerability in the Dictionary (rtgdictionary) extension 0.1.9 and earlier for TYPO3 allows attackers to execute arbitrary code via unknown vectors.	2008-12-31	10.0	CVE-2008-5801 CONFIRM
v3chat -- v3_chat_live_support	admin/index.php in V3 Chat Live Support 3.0.4 allows remote attackers to bypass authentication and gain administrative access by setting the admin cookie to 1.	2008-12-31	7.5	CVE-2008-5783 BID MILW0RM FRSIRT SECUNIA
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
v3chat -- v3_chat_profiles_dating_script	V3 Chat - Profiles/Dating Script 3.0.2 allows remote attackers to bypass authentication and gain administrative access by setting the admin cookie to 1.	2008-12-31	7.5	CVE-2008-5784 BID MILW0RM FRSIRT SECUNIA
v3chat -- v3_chat_profiles_dating_script	SQL injection vulnerability in V3 Chat - Profiles/Dating Script 3.0.2 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password fields.	2008-12-31	7.5	CVE-2008-5785 BID MILW0RM FRSIRT
zeeways -- zeematri	SQL injection vulnerability in bannerclick.php in ZeeMatri 3.0 allows remote attackers to execute arbitrary SQL commands via the adid parameter.	2008-12-31	7.5	CVE-2008-5782 BID MILW0RM FRSIRT

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
2500mhz -- worksimple	WorkSimple 1.2.1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing usernames and passwords via a direct request for data/usr.txt.	2008-12-30	5.0	CVE-2008-5765 XF BID MILW0RM SECUNIA OSVDB
bloofox -- bloofoxcms	Directory traversal vulnerability in plugins/spaw2/dialogs/dialog.php in BloofoxCMS 0.3.4 allows remote attackers to read arbitrary files via the (1) lang, (2) theme, and (3) module parameters.	2008-12-29	4.3	CVE-2008-5748 BID MILW0RM SECUNIA
bpsoft -- hex_workshop	Buffer overflow in BreakPoint Software Hex Workshop 5.1.4 allows user-assisted attackers to cause a denial of service and possibly execute arbitrary code via a long mapping reference in a Color Mapping (.cmap) file.	2008-12-30	6.8	CVE-2008-5756 BID MILW0RM
f-prot -- f-prot_antivirus	F-Prot 4.6.8 for GNU/Linux allows remote attackers to bypass anti-virus	2008-12-29	5.0	CVE-2008-5747 BID

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	protection via a crafted ELF program with a "corrupted" header that still allows the program to be executed. NOTE: due to an error in the initial disclosure, F-secure was incorrectly stated as the vendor.			BUGTRAQ BUGTRAQ BUGTRAQ MISC
flatnux -- flatnux	Cross-site scripting (XSS) vulnerability in FlatnuX CMS (aka Flatnuke3) 2008-12-11 allows remote attackers to inject arbitrary web script or HTML via the name parameter in an updaterecord action to index.php in the 08_Files module. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-12-30	4.3	CVE-2008-5759 XF SECUNIA
flatnux -- flatnux	Multiple cross-site scripting (XSS) vulnerabilities in FlatnuX CMS (aka Flatnuke3) 2008-12-11 allow remote attackers to inject arbitrary web script or HTML via (1) the mod parameter to the default URI; (2) the foto parameter to photo.php in the 05_Foto module; or (3) the name parameter in an insertrecord action to index.php in the 08_Files module, as demonstrated by injection within a SRC attribute of an IFRAME element.	2008-12-30	4.3	CVE-2008-5761 XF XF BID BID MILW0RM SECUNIA
futomi -- access_analyzer_cgi	futomi CGI Cafe Access Analyzer CGI Standard 4.0.1 and earlier and Access Analyzer CGI Professional 4.11.3 and earlier use a predictable session id, which makes it easier for remote attackers to hijack sessions, and obtain sensitive information about analysis results, via a modified id.	2009-01-02	5.8	CVE-2008-5809 CONFIRM JVNDB JVN
google -- chrome	** DISPUTED ** Argument injection vulnerability in Google Chrome 1.0.154.36 on Windows XP SP3 allows remote attackers to execute arbitrary commands via the --renderer-path option in a chromehtml: URI. NOTE: a third party	2008-12-29	6.8	CVE-2008-5749 BID BUGTRAQ BUGTRAQ MILW0RM MISC

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	disputes this issue, stating that Chrome "will ask for user permission" and "cannot launch the applet even [if] you have given out the permission."			
hostforest -- forest_blog	Forest Blog 1.3.2 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing passwords via a direct request for blog.mdb.	2008-12-30	5.0	CVE-2008-5780 XF MILW0RM
indisguise -- indiscripts_enthusiast	PHP remote file inclusion vulnerability in show_joined.php in Indiscripts Enthusiast 3.1.4, and possibly earlier, allows remote attackers to execute arbitrary PHP code via a URL in the path parameter. NOTE: the researcher also points out the analogous directory traversal issue.	2008-12-31	6.8	CVE-2008-5792 BID BUGTRAQ MILW0RM FRSIRT MISC SECUNIA
infrae -- silva infrae -- silva_find	Cross-site scripting (XSS) vulnerability in the Silva Find extension 1.1.5 and earlier in Silva 1.x before 1.6.3.2, Silva 2.0 before 2.0.12.2, and Silva 2.1 before 2.1.0.2 allows remote attackers to inject arbitrary web script or HTML via the fulltext parameter.	2008-12-31	4.3	CVE-2008-5786 CONFIRM MISC
intellitamper -- intellitamper	Stack-based buffer overflow in IntelliTamper 2.07 and 2.08 allows remote attackers to execute arbitrary code via a MAP file containing a long URL, possibly a related issue to CVE-2006-2494.	2008-12-30	6.8	CVE-2008-5755 BID MILW0RM
kerio -- kerio_mailserver	Cross-site scripting (XSS) vulnerability in error413.php in Kerio MailServer before 6.6.2 allows remote attackers to inject arbitrary web script or HTML via the sent parameter. NOTE: some of these details are obtained from third party information.	2008-12-30	4.3	CVE-2008-5760 BID
kerio -- kerio_mailserver	Multiple cross-site scripting (XSS) vulnerabilities in Kerio MailServer before 6.6.2 allow remote attackers to	2008-12-30	4.3	CVE-2008-5769 BID

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	inject arbitrary web script or HTML via the (1) folder parameter to mailCompose.php or the (2) daytime parameter to calendarEdit.php. NOTE: some of these details are obtained from third party information.			
lovecms -- lovecms	Directory traversal vulnerability in system/admin/images.php in LoveCMS 1.6.2 Final allows remote attackers to delete arbitrary files via a .. (dot dot) in the delete parameter.	2008-12-31	5.0	CVE-2008-5794 XF BID MILW0RM
mariovaldez -- simple_text-file_login_script	Simple Text-File Login Script (SiTeFiLo) 1.0.6 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing the password via a direct request for slog_users.txt.	2008-12-30	5.0	CVE-2008-5762 MILW0RM SECUNIA OSVDB
microsoft -- windows_media_player	Integer overflow in Microsoft Windows Media Player 9, 10, and 11 allows remote attackers to execute arbitrary code via a crafted (1) WAV, (2) SND, or (3) MID file. NOTE: it is not clear whether this vulnerability is related to CVE-2008-4927 or CVE-2008-2253.	2008-12-29	4.3	CVE-2008-5745 SECTRACK BID BUGTRAQ
microsoft -- internet_explorer	Argument injection vulnerability in Microsoft Internet Explorer 8 beta 2 on Windows XP SP3 allows remote attackers to execute arbitrary commands via the --renderer-path option in a chromehtml: URI.	2008-12-29	6.8	CVE-2008-5750 BID BUGTRAQ MILW0RM MISC
nukedit -- nukedit	Nukedit 4.9.8 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing usernames and passwords via a direct request for database/dbsite.mdb.	2008-12-30	5.0	CVE-2008-5773 MILW0RM SECUNIA
phparanoid -- phparanoid	Cross-site request forgery (CSRF) vulnerability in PHParanoid before 0.5	2008-12-30	6.8	CVE-2008-5758 CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	allows remote attackers to perform unspecified actions as authenticated users via unknown vectors related to private messages.			SECUNIA
phpweather -- phpweather	Cross-site scripting (XSS) vulnerability in config/make_config.php in PHP Weather 2.2.2 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2008-12-30	4.3	CVE-2008-5770 XF BID MILW0RM SECUNIA
recly -- clickheat-heatmap	Multiple PHP remote file inclusion vulnerabilities in the Clickheat - Heatmap stats (com_clickheat) component 1.0.1 for Joomla! allow remote attackers to execute arbitrary PHP code via a URL in the (1) GLOBALS[mosConfig_absolute_path] parameter to (a) install.clickheat.php, (b) Cache.php and (c) Clickheat_Heatmap.php in Recly/Clickheat/, and (d) Recly/common/GlobalVariables.php; and the (2) mosConfig_absolute_path parameter to (e) _main.php and (f) main.php in includes/heatmap, and (g) includes/overview/main.php.	2008-12-31	6.8	CVE-2008-5793 XF BID MILW0RM
six_apart -- movable_type sixapart -- movable_type	Cross-site scripting (XSS) vulnerability in Six Apart Movable Type Enterprise (MTE) 1.x before 1.56; Movable Type (MT) 3.x before 3.38; and Movable Type, Movable Type Open Source (MTOS), and Movable Type Enterprise 4.x before 4.23 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, possibly related to "application management."	2009-01-02	4.3	CVE-2008-5808 BID CONFIRM SECUNIA JVNDB JVN
sun -- snmp_management_agent	Sun SNMP Management Agent (SUNWmasf) 1.4u2 through 1.5.4 allows local users to overwrite arbitrary files and gain privileges via a symlink attack on temporary files.	2008-12-29	6.9	CVE-2008-5746 SECTRACK BID SUNALERT SECUNIA

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
teamst -- testlink	Multiple cross-site scripting (XSS) vulnerabilities in TestLink before 1.8 RC1 allow remote attackers to inject arbitrary web script or HTML via (1) Testproject Names and (2) Testplan Names in planEdit.php, and possibly (3) Testcaseprefixes in projectview.tpl.	2008-12-31	4.3	CVE-2008-5807 XF BID CONFIRM SECUNIA
typo3 -- eluna_page_comments_extension	Cross-site scripting (XSS) vulnerability in the eluna Page Comments (eluna_pagecomments) extension 1.1.2 and earlier for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-12-31	4.3	CVE-2008-5795 BID CONFIRM SECUNIA
typo3 -- wir_ber_uns_extension	Cross-site scripting (XSS) vulnerability in the Wir ber uns [sic] (fsmi_people) extension 0.0.24 and earlier for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-12-31	4.3	CVE-2008-5799 CONFIRM
wordpress -- page_flip_image_gallery_plugin	Directory traversal vulnerability in getConfig.php in the Page Flip Image Gallery plugin 0.2.2 and earlier for WordPress, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the book_id parameter. NOTE: some of these details are obtained from third party information.	2008-12-30	4.3	CVE-2008-5752 XF BID MILW0RM SECUNIA OSVDB
Back to top				

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
arabportal -- arab_portal	Directory traversal vulnerability in mod.php in Arab Portal 2.1 on Windows allows remote attackers to read arbitrary files via a .. (dot dot) in the file parameter, in conjunction with a show action.	2008-12-31	2.6	CVE-2008-5787 XF BID BUGTRAQ MILW0RM SECUNIA
textpattern -- textpattern	Cross-site scripting (XSS) vulnerability in textarea/index.php in Textpattern (aka Txp CMS)	2008-12-30	3.5	CVE-2008-5757 BID
Back to top				

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	4.0.6 and earlier allows remote authenticated users to inject arbitrary web script or HTML via the Body parameter in an article action. NOTE: some of these details are obtained from third party information.			BUGTRAQ SECUNIA
Back to top				