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 (CVSS Score: 7.0 .. 10.0)				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
IPureServer -- S.T.A.L.K.E.R.	Stack-based buffer overflow in the IPureServer::_Recieve function in S.T.A.L.K.E.R.: Shadow of Chernobyl 1.0006 and earlier allows remote attackers to execute arbitrary code via a compressed 0x39 packet, which is decompressed by the NET_Compressor::Decompress function.	2009-04-10	10.0	CVE-2008-6703 XF BUGTRAQ SECUNIA OSVDB MISC
acutecp -- acute_control_panel	Multiple PHP remote file inclusion vulnerabilities in Acute Control Panel 1.0.0 allow remote attackers to execute arbitrary PHP code via a URL in the theme_directory parameter to (1) container.php and (2) header.php in themes/.	2009-04-06	7.5	CVE-2009-1248 XF BID MILW0RM SECUNIA
acutecp.rediscussed -- acutecp	SQL injection vulnerability in login.php in Acute Control Panel 1.0.0 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-04-06	7.5	CVE-2009-1247 XF BID MILW0RM SECUNIA
beaussier -- roomphplanning	SQL injection vulnerability in RoomPHPlanning 1.5 allows remote attackers to execute arbitrary SQL commands via the idresa parameter to resaopen.php.	2009-04-07	7.5	CVE-2008-6633 XF VUPEN BID MILW0RM SECUNIA
beaussier -- roomphplanning	SQL injection vulnerability in RoomPHPlanning 1.5 allows remote attackers to execute arbitrary SQL commands via the idroom parameter to weekview.php.	2009-04-07	7.5	CVE-2008-6634 XF BID MILW0RM SECUNIA
cclamav -- clamav clamav -- clamav clamavclamav -- 0.11 clamavclamav -- 0.80_rc4	libclamav/untar.c in ClamAV before 0.95 allows remote attackers to cause a denial of service (infinite loop) via a crafted file that causes (1) clamd and (2) clamscan to	2009-04-08	7.8	CVE-2009-1270 CONFIRM

clamavclamav -- 0.80_rc4 clamavs -- clamav	hang.			MLIST
cisco -- adaptive_security_appliance_5500 cisco -- pix	Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.1(1) through 7.1(2)82, 7.2 before 7.2(4)27, 8.0 before 8.0(4)25, and 8.1 before 8.1(2)15, when AAA override-account-disable is entered in a general-attributes field, allow remote attackers to bypass authentication and establish a VPN session to an ASA device via unspecified vectors.	2009-04-09	7.8	CVE-2009-1155 CISCO
cisco -- adaptive_security_appliance_5500 cisco -- pix	Memory leak on Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.0 before 7.0(8)6, 7.1 before 7.1(2)82, 7.2 before 7.2(4)30, 8.0 before 8.0(4)28, and 8.1 before 8.1(2)19 allows remote attackers to cause a denial of service (memory consumption or device reload) via a crafted TCP packet.	2009-04-09	7.8	CVE-2009-1157 CISCO
cisco -- adaptive_security_appliance_5500 cisco -- pix	Unspecified vulnerability on Cisco Adaptive Security Appliances (ASA) 5500 Series devices 7.0 before 7.0(8)6, 7.1 before 7.1(2)82, 7.2 before 7.2(4)26, 8.0 before 8.0(4)24, and 8.1 before 8.1(2)14, when H.323 inspection is enabled, allows remote attackers to cause a denial of service (device reload) via a crafted H.323 packet.	2009-04-09	7.8	CVE-2009-1158 CISCO
cisco -- adaptive_security_appliance_5500 cisco -- pix	Unspecified vulnerability on Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.2 before 7.2(4)26, 8.0 before 8.0(4)22, and 8.1 before 8.1(2)12, when SQL*Net inspection is enabled, allows remote attackers to cause a denial of service (traceback and device reload) via a series of SQL*Net packets.	2009-04-09	7.8	CVE-2009-1159 CISCO
clam_anti-virus -- clamav clamav -- clamav	Unspecified vulnerability in ClamAV before 0.95 allows remote attackers to bypass detection of malware via a modified RAR archive.	2009-04-03	7.5	CVE-2009-1241 BID BUGTRAQ MLIST MISC
class-systems -- class_systems	Unrestricted file upload vulnerability in class/ApplyDB.php in ClassSystem 2.3 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in class/UploadHomepage/.	2009-04-06	7.5	CVE-2008-6619 XF VUPEN BID BUGTRAQ MISC SECUNIA
diocese_of_portsmouth -- pd_calendar_today typo3 -- typo3	SQL injection vulnerability in Diocese of Portsmouth Calendar Today (pd_calendar_today) extension 0.0.3 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-04-10	7.5	CVE-2008-6691 CONFIRM
dirk_bartley -- nweb2fax	viewrq.php in nweb2fax 0.2.7 and earlier allows remote attackers to execute arbitrary code via shell metacharacters in the var_filename parameter in a (1) tif or (2) pdf format action.	2009-04-08	7.5	CVE-2008-6669 XF BID MILW0RM
dotcontent -- fluentcms	SQL injection vulnerability in view.php in DotContent FluentCMS 4.x allows remote attackers to execute arbitrary SQL commands via the sid parameter. NOTE: some of these details are obtained from third party information.	2009-04-07	7.5	CVE-2008-6642 XF BID MILW0RM SECUNIA
ezbsystems -- ultraiso	Multiple stack-based buffer overflows in UltraISO 9.3.3.2685 and earlier allow remote attackers to cause a denial of service (crash) or execute arbitrary code via a	2009-04-07	9.0	CVE-2009-1260 XF VUPEN MILW0RM

	crafted (1) CCD or (2) IMG file.			MILW0RM SECUNIA OSVDB
flexcms -- flexcms	SQL injection vulnerability in FlexCMS 2.5 allows remote attackers to execute arbitrary SQL commands via the ItemId parameter. NOTE: some of these details are obtained from third party information.	2009-04-07	7.5	CVE-2009-1256 XF BID MILW0RM
fortinet -- forticlient	Format string vulnerability in Fortinet FortiClient 3.0.614, and possibly earlier, allows local users to execute arbitrary code via format string specifiers in the VPN connection name.	2009-04-07	7.2	CVE-2009-1262 XF VUPEN SECTRACK BUGTRAQ MISC SECUNIA OSVDB FULLDISC
fr.simon_rundell -- pd_trainingcourses	SQL injection vulnerability in Diocese of Portsmouth Training Courses (pd_trainingcourses) extension 0.1.1 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-04-10	7.5	CVE-2008-6692 CONFIRM
fr.simon_rundell -- ste_prayer	SQL injection vulnerability in Random Prayer (ste_prayer) 0.0.1 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-04-10	7.5	CVE-2008-6694 CONFIRM
frank_naegler -- timtab_sociable	SQL injection vulnerability in TIMTAB social bookmark icons (timtab_sociable) 2.0.4 and earlier extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-04-10	7.5	CVE-2008-6695 CONFIRM
geody -- dagger	SQL injection vulnerability in skins/default.php in Geody Labs Dagger - The Cutting Edge r12feb2008, when register_globals is enabled, allows remote attackers to execute arbitrary SQL commands via the dir_inc parameter.	2009-04-07	7.5	CVE-2008-6635 BID MILW0RM SECUNIA
ghostscript -- ghostscript	The CCITTFax decoding filter in Ghostscript 8.60, 8.61, and possibly other versions, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PDF file that triggers a buffer underflow in the cf_decode_2d function.	2009-04-08	7.5	CVE-2007-6725 CONFIRM CONFIRM MLIST FEDORA
glfusion -- glfusion	SQL injection vulnerability in private/system/lib-session.php in glFusion 1.1.2 and earlier allows remote attackers to execute arbitrary SQL commands via the glf_session cookie parameter.	2009-04-09	7.5	CVE-2009-1282 BID CONFIRM
graphicsmagick -- graphicsmagick	Unspecified vulnerability in GraphicsMagick before 1.2.3 allows remote attackers to cause a denial of service (crash) via unspecified vectors in DPX images. NOTE: some of these details are obtained from third party information.	2009-04-06	7.8	CVE-2008-6621 VUPEN CONFIRM SECUNIA CONFIRM
gravityboardx -- gravity_board_x	SQL injection vulnerability in index.php in Gravity Board X (GBX) 2.0 BETA allows remote attackers to execute arbitrary SQL commands via the member_id parameter in a viewprofile action. NOTE: the board_id issue is already covered by CVE-2008-2996.2.	2009-04-09	7.5	CVE-2009-1277 XF BID MILW0RM
gravityboardx -- gravity_board_x	Static code injection vulnerability in forms/ajax/configure.php in Gravity Board X (GBX) 2.0 BETA allows remote attackers to inject arbitrary PHP code into config.php via the configure action to index.php.	2009-04-09	7.5	CVE-2009-1278 XF BID MILW0RM
				CVE-2008-

impliedbydesign -- ibd_micro_cms	Multiple SQL injection vulnerabilities in microcms-admin-login.php in Implied By Design (IBD) Micro CMS 3.5 allow remote attackers to execute arbitrary SQL commands via the (1) Username and (2) Password fields.	2009-04-06	7.5	6614 XF MISC BID MISC
insanevisions -- onecms	SQL injection vulnerability in asd.php in OneCMS 2.5 allows remote attackers to execute arbitrary SQL commands via the sitename parameter.	2009-04-07	7.5	CVE-2008-6652 XF BID MILW0RM
irfanview -- formats	Integer overflow in the FORMATS Plugin before 4.23 for IrfanView allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a large XPM file that triggers a heap-based buffer overflow.	2009-04-09	9.3	CVE-2009-0197 XF VUPEN CONFIRM
janbednarik -- cooluri typo3 -- typo3	SQL injection vulnerability in CoolURI (cooluri) 1.0.11 and earlier extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-04-10	7.5	CVE-2008-6686 CONFIRM
joomla -- joomla rd-media -- rd-autos	SQL injection vulnerability in the RD-Autos (com_rdautos) component 1.5.7 for Joomla! allows remote attackers to execute arbitrary SQL commands via the makeid parameter in index.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-07	7.5	CVE-2009-1258 XF BID SECUNIA OSVDB
kevin_renskers -- dmmjobcontrol	SQL injection vulnerability in JobControl (dmmjobcontrol) 1.15.0 and earlier extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-04-10	7.5	CVE-2008-6689 CONFIRM
ktools -- photostore	SQL injection vulnerability in gallery.php in Ktools PhotoStore 3.4.3 allows remote attackers to execute arbitrary SQL commands via the gid parameter.	2009-04-07	7.5	CVE-2008-6647 XF BID MILW0RM SECUNIA
ktools -- photostore	SQL injection vulnerability in crumbs.php in Ktools PhotoStore 3.4.3 and 3.5.2 allows remote attackers to execute arbitrary SQL commands via the gid parameter to about_us.php. NOTE: this might be the same issue as CVE-2008-6647.	2009-04-07	7.5	CVE-2008-6648 XF BID MILW0RM SECUNIA
ktools -- photostore	SQL injection vulnerability in manager/image_details_editor.php in Ktools PhotoStore 2.5, 2.9.8, 3.1.0, and other versions through 3.5.2 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-04-07	7.5	CVE-2008-6649 XF BID MILW0RM SECUNIA
linux -- linux openafs -- openafs	The cache manager in the client in OpenAFS 1.0 through 1.4.8 and 1.5.0 through 1.5.58 on Linux allows remote attackers to cause a denial of service (system crash) via an RX response with a large error-code value that is interpreted as a pointer and dereferenced, related to use of the ERR_PTR macro.	2009-04-08	7.8	CVE-2009-1250 BID CONFIRM CONFIRM
magic_iso_maker -- magic_iso_maker	Heap-based buffer overflow in Magic ISO Maker 5.5 build 0274 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted CCD file.	2009-04-07	9.0	CVE-2009-1257 XF VUPEN MILW0RM SECUNIA OSVDB
manu_oehler -- toto	SQL injection vulnerability in Fussballtippspiel (toto) 0.1.1 and earlier extension for TYPO3 allows remote	2009-04-	7.5	CVE-2008-6696

typo3 -- typo3	attackers to execute arbitrary SQL commands via unknown vectors.	10	7.5	6696 CONFIRM
marc_melvin -- a_php_scripts_news_management_system	A+ PHP Scripts News Management System (NMS) allows remote attackers to bypass authentication and gain administrator privileges by setting the mobsuser and mobspass cookies to 1.	2009-04-08	7.5	CVE-2008-6667 BID MILW0RM
mercuryboard -- mercuryboard	SQL injection vulnerability in func/login.php in MercuryBoard 1.1.5 and earlier allows remote attackers to execute arbitrary SQL commands via the User-Agent HTTP header ($_SERVER['HTTP_USER_AGENT']).	2009-04-07	7.5	CVE-2008-6632 XF BID MILW0RM
michael_fritz -- worldcup	SQL injection vulnerability in TARGET-E WorldCup Bets (worldcup) 2.0.0 and earlier extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-04-10	7.5	CVE-2008-6697 CONFIRM
mit -- kerberos	The asn1_decode_generaltime function in lib/krb5/asn.1/asn1_decode.c in the ASN.1 GeneralizedTime decoder in MIT Kerberos 5 (aka krb5) before 1.6.4 allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via vectors involving an invalid DER encoding that triggers a free of an uninitialized pointer.	2009-04-08	10.0	CVE-2009-0846 CONFIRM
netlab -- classsystem	Multiple SQL injection vulnerabilities in ClassSystem 2.3 allow remote attackers to execute arbitrary SQL commands via the teacher_id parameter in (1) class/HomepageMain.php and (2) class/HomepageTop.php, and (3) the message_id parameter in class/MessageReply.php.	2009-04-06	7.5	CVE-2008-6618 XF VUPEN BID BUGTRAQ MISC SECUNIA
netscout -- ngenius_infinistream netscout -- visualizer	NetScout (formerly Network General) Visualizer V2100 and InfiniStream i1730 do not restrict access to ResourceManager/en_US/domains/add_domain.jsp, which allows remote attackers to gain administrator privileges via a direct request.	2009-04-10	7.5	CVE-2008-6701 XF BUGTRAQ SECUNIA OSVDB
nikola_arezina -- com_bookjoomlas	SQL injection vulnerability in sub_commententry.php in the BookJoomlas (com_bookjoomlas) component 0.1 for Joomla! allows remote attackers to execute arbitrary SQL commands via the gbid parameter in a comment action to index.php.	2009-04-07	7.5	CVE-2009-1263 XF VUPEN BID MILW0RM
openafs -- openafs unix -- unix	Heap-based buffer overflow in the cache manager in the client in OpenAFS 1.0 through 1.4.8 and 1.5.0 through 1.5.58 on Unix platforms allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via an RX response containing more data than specified in a request, related to use of XDR arrays.	2009-04-08	10.0	CVE-2009-1251 CONFIRM
openautoclassifieds -- open_auto_classifieds	Multiple SQL injection vulnerabilities in Open Auto Classifieds 1.4.3b allow remote attackers to execute arbitrary SQL commands via (1) the id parameter to listings.php and (2) the username field to login.php.	2009-04-07	7.5	CVE-2008-6656 XF BID MILW0RM
oxyproject -- oxybox	Static code injection vulnerability in edithistory.php in OxYProject OxYBox 0.85 allows remote attackers to inject arbitrary PHP code into oxyhistory.php via the oxymsg parameter.	2009-04-07	10.0	CVE-2008-6651 XF BID MILW0RM
phpauctions -- phpauction	SQL injection vulnerability in profile.php in PHPAuctions.info PHPAuctions (aka PHPAuctionSystem) allows remote attackers to execute	2009-04-08	7.5	CVE-2008-6663 XF

	arbitrary SQL commands via the auction_id parameter, a different vector than CVE-2009-0106.	08		BID MILW0RM
quickersite -- quickersite	Unrestricted file upload vulnerability in fckeditor251/editor/filemanager/connectors/asp/upload.asp in QuickerSite 1.8.5 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file.	2009-04-08	7.5	CVE-2008-6677 MISC MISC SECUNIA
quickersite -- quickersite	SQL injection vulnerability in asp/includes/contact.asp in QuickerSite 1.8.5 allows remote attackers to execute arbitrary SQL commands via the sNickName parameter in a profile action to default.asp.	2009-04-08	7.5	CVE-2008-6678 MISC MISC SECUNIA
sebastian_baumann -- sb_downloader typo3 -- typo3	SQL injection vulnerability in Download system (sb_downloader) extension 0.1.4 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-04-10	7.5	CVE-2008-6693 CONFIRM
thomas_waggershauser -- air_filemanager	Unspecified vulnerability in Frontend Filemanager (air_filemanager) 0.6.1 and earlier extension for TYPO3 allows remote attackers to execute arbitrary commands via unknown vectors.	2009-04-10	7.5	CVE-2008-6685 CONFIRM
typo3 -- nd_antispam	Unspecified vulnerability in nepa-design.de Spam Protection (nd_antispam) extension 1.0.3 for TYPO3 allows remote attackers to modify configuration via unknown vectors.	2009-04-10	7.5	CVE-2008-6690 CONFIRM
versalsoft -- http_file_upload_activex_control	Insecure method vulnerability in the Versalsoft HTTP Image Uploader ActiveX control (UUploaderSvrD.dll 6.0.0.35) allows remote attackers to delete arbitrary files via the RemoveFileOrDir method.	2009-04-07	8.8	CVE-2008-6638 XF BID MILW0RM
vertex4 -- sunage	Vertex4 SunAge 1.08.1 and earlier allows remote attackers to cause a denial of service (infinite loop and hang) via a crafted join packet to UDP port 27960.	2009-04-08	7.8	CVE-2008-6671 XF VUPEN BID SECUNIA OSVDB MISC MISC
vmware -- ace vmware -- player vmware -- server vmware -- workstation	Heap-based buffer overflow in the VNnc Codec in VMware Workstation 6.5.x before 6.5.2 build 156735, VMware Player 2.5.x before 2.5.2 build 156735, VMware ACE 2.5.x before 2.5.2 build 156735, and VMware Server 2.0.x before 2.0.1 build 156745 allows remote attackers to execute arbitrary code via a crafted web page or video file, aka ZDI-CVE-435.	2009-04-06	9.3	CVE-2009-0909 FULLDISC MLIST
webbdomain -- post_card	SQL injection vulnerability in getin.php in WEBBDOMAIN Post Card (aka Web Postcards) 1.02 and earlier allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-04-06	7.5	CVE-2008-6623 XF BID MILW0RM SECUNIA OSVDB
webbdomain -- petition	SQL injection vulnerability in getin.php in WEBBDOMAIN Petition 1.02, 2.0, and 3.0 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-04-06	7.5	CVE-2008-6624 XF BID MILW0RM OSVDB
webbdomain -- polls	SQL injection vulnerability in getin.php in WEBBDOMAIN Polls (aka Poll) 1.0 and 1.01 allows	2009-04-	7.5	CVE-2008-6625 XF BID

webbdomain -- polls	remote attackers to execute arbitrary SQL commands via the username parameter.	06	7.5	BID MILW0RM SECUNIA OSVDB
webbdomain -- quiz	SQL injection vulnerability in getin.php in WEBBDOMAIN Quiz 1.02 and earlier allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-04-06	7.5	CVE-2008-6626 XF BID MILW0RM SECUNIA OSVDB
webbdomain -- web_shop	SQL injection vulnerability in getin.php in WEBBDOMAIN WebShop 1.2, 1.1, 1.02, and earlier allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-04-06	7.5	CVE-2008-6627 XF BID MILW0RM SECUNIA OSVDB
webbdomain -- web_shop_online	SQL injection vulnerability in detail.php in WEBBDOMAIN Multi Languages WebShop Online 1.02 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-04-06	7.5	CVE-2008-6628 MILW0RM SECUNIA OSVDB
webbdomian -- post_card	SQL injection vulnerability in choosecard.php in WEBBDOMAIN Post Card (aka Web Postcards) 1.02, 1.01, and earlier allows remote attackers to execute arbitrary SQL commands via the catid parameter.	2009-04-06	7.5	CVE-2008-6622 BID MILW0RM SECUNIA OSVDB
wh-com -- com_webhosting	SQL injection vulnerability in webhosting.php in the Webhosting Component (com_webhosting) module before 1.1 RC7 for Joomla! and Mambo allows remote attackers to execute arbitrary SQL commands via the catid parameter to index.php.	2009-04-07	7.5	CVE-2008-6653 XF BID MILW0RM CONFIRM
yarck -- sh-news	action.php in SH-News 3.0 allows remote attackers to bypass authentication and gain administrator privileges by setting the shuser and shpass cookies to non-zero values.	2009-04-08	7.5	CVE-2008-6664 XF MISC BID MILW0RM
zen-cart -- zen_cart	SQL injection vulnerability in index.php in Zen Software Zen Cart 2008 allows remote attackers to execute arbitrary SQL commands via the keyword parameter in the advanced_search_result page. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-06	7.5	CVE-2008-6615 XF BID MISC

Back to top

Medium Vulnerabilities (CVSS Score: 4.0 .. 6.9)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
S.T.A.L.K.E.R.: Shadow of Chernobyl	S.T.A.L.K.E.R.: Shadow of Chernobyl 1.0006 and earlier allows remote attackers to cause a denial of service (crash) via a long nickname, which triggers an exception.	2009-04-10	5.0	CVE-2008-6702 XF SECUNIA OSVDB MISC
ajaxplorer -- ajaxplorer	Cross-site request forgery (CSRF) vulnerability in admin.php in AjaXplorer 2.3.3 and 2.3.4 allows remote attackers to hijack the authentication of administrators	2009-04-07	6.8	CVE-2008-6639 XF OSVDB

	for requests that modify passwords via the update_user_pwd action.	07		OSVDB SECUNIA MISC
alexeyozerov -- bigdump	Unrestricted file upload vulnerability in bigdump.php in Alexey Ozerov BigDump 0.29b allows remote attackers to execute arbitrary code by uploading a file with an executable extension followed by a .sql extension, then accessing this file via a direct request. NOTE: some of these details are obtained from third party information.	2009-04-07	6.5	CVE-2008-6660 XF BID BUGTRAQ
anantasoft -- ananta_cms	change.php in Ananta CMS 1.0b5, with magic_quotes_gpc disabled, allows remote attackers to gain administrator privileges via a crafted email parameter, possibly related to code injection.	2009-04-08	6.8	CVE-2008-6665 XF BID MILW0RM
andrew_j.korty -- pam_ssh	pam_ssh 1.92 and possibly other versions, as used when PAM is compiled with USE=ssh, generates different error messages depending on whether the username is valid or invalid, which makes it easier for remote attackers to enumerate usernames.	2009-04-08	5.0	CVE-2009-1273 SECUNIA CONFIRM
apache -- struts dojotoolkit -- dojo	Multiple cross-site scripting (XSS) vulnerabilities in Dojo 0.4.1 and 0.4.2, as used in Apache Struts and other products, allow remote attackers to inject arbitrary web script or HTML via unspecified vectors involving (1) xip_client.html and (2) xip_server.html in src/io/.	2009-04-09	4.3	CVE-2007-6726 CONFIRM CONFIRM CONFIRM
apache -- struts	Cross-site scripting (XSS) vulnerability in Apache Struts before 1.2.9-162.31.1 on SUSE Linux Enterprise (SLE) 11, before 1.2.9-108.2 on SUSE openSUSE 10.3, before 1.2.9-198.2 on SUSE openSUSE 11.0, and before 1.2.9-162.163.2 on SUSE openSUSE 11.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to "insufficient quoting of parameters."	2009-04-09	4.3	CVE-2008-2025 CONFIRM
apache -- struts	Multiple cross-site scripting (XSS) vulnerabilities in Apache Struts 2.0.x before 2.0.11.1 and 2.1.x before 2.1.1 allow remote attackers to inject arbitrary web script or HTML via vectors associated with improper handling of (1) " (double quote) characters in the href attribute of an s:a tag and (2) parameters in the action attribute of an s:url tag.	2009-04-09	4.3	CVE-2008-6682 CONFIRM CONFIRM
apache -- tiles	Apache Tiles 2.1 before 2.1.2, as used in Apache Struts and other products, evaluates Expression Language (EL) expressions twice in certain circumstances, which allows remote attackers to conduct cross-site scripting (XSS) attacks or obtain sensitive information via unspecified vectors, related to the (1) tiles:putAttribute and (2) tiles:insertTemplate JSP tags.	2009-04-09	6.8	CVE-2009-1275 CONFIRM CONFIRM
aspindir -- shader_tv	Multiple SQL injection vulnerabilities in Shader TV (Beta) allow remote authenticated administrators to execute arbitrary SQL commands via the sid parameter to (1) kanal.asp, (2) google.asp, and (3) hakk.asp in yonet/; and allow remote attackers to execute arbitrary SQL commands via the (4) username or (5) password fields to yonet/default.asp.	2009-04-07	6.5	CVE-2008-6641 XF BID MILW0RM
avg -- avg_anti-virus	AVG Anti-Virus for Linux 7.5.51, and possibly earlier, allows remote attackers to cause a denial of service (segmentation fault) or possibly execute arbitrary code via a malformed UPX compressed file, which triggers memory corruption.	2009-04-07	4.3	CVE-2008-6662 XF VUPEN BID OSVDB MISC BUGTRAQ
batman -- batmanportal	Multiple SQL injection vulnerabilities in BatmanPorTaL allow remote attackers to execute arbitrary SQL commands via the id parameter to (1) uyeadmin.asp and (2) profil.asp. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-07	6.4	CVE-2008-6640 XF MISC BID
bibtex -- bibtex	Buffer overflow in BibTeX 0.99 allows context-dependent attackers to cause a denial of service (memory corruption and crash) via a long .bib bibliography file.	2009-04-09	5.0	CVE-2009-1284 CONFIRM MLIST CONFIRM
				CVE-2008-

bitdefender -- bitdefender_antivirus	Multiple integer overflows in the scanning engine in Bitdefender for Linux 7.60825 and earlier allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a malformed (1) NeoLite and (2) ASProtect packed PE file.	2009-04-07	5.0	6661 XF VUPEN BID OSVDB MISC SECUNIA BUGTRAQ
blogphp -- blogphp	Multiple cross-site scripting (XSS) vulnerabilities in index.php in BlogPHP 2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) user parameter in a sendmessage action and the (2) username parameter when registering a new user, different vectors than CVE-2008-0679.	2009-04-07	4.3	CVE-2008-6631 XF XF BID MISC SECUNIA
butterflymedia -- butterfly_organizer	Multiple cross-site scripting (XSS) vulnerabilities in Butterfly Organizer 2.0.0 allow remote attackers to inject arbitrary web script or HTML via the (1) mytable parameter to view.php, (2) mytable parameter to viewdb2.php, (3) tablehere parameter to category-rename.php, and (4) letter parameter to module-contacts.php.	2009-04-10	4.3	CVE-2008-6700 XF BID MILW0RM
cisco -- adaptive_security_appliance_5500 cisco -- pix	Unspecified vulnerability on Cisco Adaptive Security Appliances (ASA) 5500 Series devices 8.0 before 8.0(4)25 and 8.1 before 8.1(2)15, when an SSL VPN or ASDM access is configured, allows remote attackers to cause a denial of service (device reload) via a crafted (1) SSL or (2) HTTP packet.	2009-04-09	5.7	CVE-2009-1156 CISCO
cisco -- adaptive_security_appliance_5500 cisco -- pix	Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.0 before 7.0(8)1, 7.1 before 7.1(2)74, 7.2 before 7.2(4)9, and 8.0 before 8.0(4)5 do not properly implement the implicit deny statement, which might allow remote attackers to successfully send packets that bypass intended access restrictions, aka Bug ID CSCsq91277.	2009-04-09	4.3	CVE-2009-1160 CISCO
clamav -- clamav	libclamav/pe.c in ClamAV before 0.95 allows remote attackers to cause a denial of service (crash) via a crafted EXE file that triggers a divide-by-zero error.	2009-04-08	5.0	CVE-2008-6680 CONFIRM MLIST
comscripts -- gedcom_to_mysl	Multiple cross-site scripting (XSS) vulnerabilities in GEDCOM_TO_MYSQL 2 allow remote attackers to inject arbitrary web script or HTML via the (1) nom_branche and (2) nom parameters to php/prenom.php; the (3) nom_branche parameter to php/index.php; and the (4) nom_branche, (5) nom, and (6) prenom parameters to php/info.php.	2009-04-07	4.3	CVE-2008-6655 XF MISC BID
coronamatrix -- phpaddressbook	Cross-site scripting (XSS) vulnerability in index.php in CoronaMatrix phpAddressBook 2.0 allows remote attackers to inject arbitrary web script or HTML via the username parameter.	2009-04-07	4.3	CVE-2008-6646 XF BID BUGTRAQ
david_cadu -- dcdgooglemap	Cross-site scripting (XSS) vulnerability in DCD GoogleMap (dcdgooglemap) 1.1.0 and earlier extension for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2009-04-10	4.3	CVE-2008-6687 CONFIRM
dirk_bartley -- nweb2fax	Multiple directory traversal vulnerabilities in nweb2fax 0.2.7 and earlier allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) id parameter to comm.php and (2) var_filename parameter to viewrq.php.	2009-04-08	5.0	CVE-2008-6668 XF XF BID MILW0RM
dojotoolkit -- dojo	Cross-site scripting (XSS) vulnerability in dijit.Editor in Dojo before 1.1 allows remote attackers to inject arbitrary web script or HTML via XML entities in a TEXTAREA element.	2009-04-09	4.3	CVE-2008-6681 CONFIRM MISC
dotnetnuke -- dotnetnuke	Cross-site scripting (XSS) vulnerability in Default.aspx in DotNetNuke 4.8.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2009-04-07	4.3	CVE-2008-6644 XF BID BUGTRAQ

drupal -- feedapi_mapper	Cross-site scripting (XSS) vulnerability in Feed element mapper 5.x before 5.x-1.1, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via the content title in admin/content/node-type/nodetype/map.	2009-04-06	4.3	CVE-2009-1249 CONFIRM CONFIRM
foolabs -- xpdf	Untrusted search path vulnerability in the Gentoo package of Xpdf before 3.02-r2 allows local users to gain privileges via a Trojan horse xpdfrc file in the current working directory, related to an unset SYSTEM_XPDFRC macro in a Gentoo build process that uses the poppler library.	2009-04-09	6.9	CVE-2009-1144 BID GENTOO SECUNIA CONFIRM CONFIRM
geody -- dagger	SQL injection vulnerability in skins/default.php in Geody Labs Dagger - The Cutting Edge r12feb2008, when register_globals is enabled, allows remote attackers to execute arbitrary SQL commands via the dir_edge_skins parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-07	6.8	CVE-2008-6636 MILW0RM SECUNIA
ghostscript -- ghostscript	Buffer overflow in the BaseFont writer module in Ghostscript 8.62, and possibly other versions, allows remote attackers to cause a denial of service (ps2pdf crash) and possibly execute arbitrary code via a crafted Postscript file.	2009-04-08	5.0	CVE-2008-6679 CONFIRM MLIST CONFIRM
glfusion -- glfusion	Cross-site scripting (XSS) vulnerability in glFusion before 1.1.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-04-09	4.3	CVE-2009-1281 CONFIRM
glfusion -- glfusion	glFusion before 1.1.3 performs authentication with a user-provided password hash instead of a password, which allows remote attackers to gain privileges by obtaining the hash and using it in the glf_password cookie, aka "User Masquerading." NOTE: this can be leveraged with a separate SQL injection vulnerability to steal hashes.	2009-04-09	6.8	CVE-2009-1283 CONFIRM
grafxsoftware -- minicwb	Multiple cross-site scripting (XSS) vulnerabilities in javascript/editor/editor/filemanager/browser/mcpuk/connectors/php/connector.php in GraFX miniCWB 2.1.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) errcontext, (2) _GET, (3) _POST, (4) _SESSION, (5) _SERVER, and (6) fckphp_config[Debug_SERVER] parameters.	2009-04-06	4.3	CVE-2008-6620 XF BID SECUNIA BUGTRAQ
ibm -- db2	IBM DB2 9.1 before FP7 returns incorrect query results in certain situations related to the order of application of an INNER JOIN predicate and an OUTER JOIN predicate, which might allow attackers to obtain sensitive information via a crafted query.	2009-04-03	5.0	CVE-2009-1239 CONFIRM AIXAPAR
insane_visions -- adaptbb	SQL injection vulnerability in inc/bb/topic.php in Insane Visions AdaptBB 1.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the topic_id parameter in a topic action to index.php.	2009-04-07	6.8	CVE-2009-1259 XF BID MILW0RM
james_stone -- tunapie	James Stone Tunapie 2.1 allows local users to overwrite arbitrary files via a symlink attack on an unspecified temporary file.	2009-04-08	4.4	CVE-2009-1253 CONFIRM CONFIRM BID DEBIAN
james_stone -- tunapie	James Stone Tunapie 2.1 allows remote attackers to execute arbitrary commands via shell metacharacters in a stream URL.	2009-04-08	6.8	CVE-2009-1254 CONFIRM CONFIRM BID DEBIAN
joomla -- joomla	Multiple cross-site request forgery (CSRF) vulnerabilities in the com_media component for Joomla! 1.5.x through 1.5.9 allow remote attackers to hijack the authentication of unspecified victims via unknown vectors.	2009-04-09	6.8	CVE-2009-1280 XF SECUNIA CONFIRM

kernel -- linux	Integer overflow in rose_sendmsg (sys/net/af_rose.c) in the Linux kernel 2.6.24.4, and other versions before 2.6.30-rc1, might allow remote attackers to obtain sensitive information via a large length value, which causes "garbage" memory to be sent.	2009-04-07	5.0	CVE-2009-1265 MLIST CONFIRM MISC
kevin_renskers -- dmmjobcontrol	Cross-site scripting (XSS) vulnerability in JobControl (dmmjobcontrol) 1.15.0 and earlier extension for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2009-04-10	4.3	CVE-2008-6688 CONFIRM
kronos -- kronos_webta	Multiple cross-site scripting (XSS) vulnerabilities in Kronos webTA allow remote attackers to inject arbitrary web script or HTML via the description field to (1) servlet/com.threeis.webta.H710selProject and (2) servlet/com.threeis.webta.H720editProjectInfo. NOTE: BID:29610 states that the initial report was incorrect, but the reason for this conclusion is unknown.	2009-04-08	4.3	CVE-2008-6666 XF BID BUGTRAQ SECUNIA OSVDB OSVDB
libraryvideocompany -- safari_montage	Multiple cross-site scripting (XSS) vulnerabilities in forgotPW.php in Library Video Company SAFARI Montage 3.1.x allow remote attackers to inject arbitrary web script or HTML via the (1) school and (2) email parameters.	2009-04-07	4.3	CVE-2008-6637 XF VUPEN BID MISC SECUNIA
littlecms -- lcms sun -- openjdk	cmsxform.c in LittleCMS (aka lcms or liblcms) 1.18, as used in OpenJDK and other products, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted image that triggers execution of incorrect code for "transformations of monochrome profiles."	2009-04-09	4.3	CVE-2009-0793 REDHAT CONFIRM VUPEN VUPEN BID BID SECUNIA SECUNIA
lokicms -- lokicms	LokiCMS 0.3.4 and possibly earlier versions does not properly restrict access to administrative functions, which allows remote attackers to bypass intended restrictions and modify configuration settings via the LokiACTION parameter in a direct request to admin.php.	2009-04-07	5.0	CVE-2008-6643 XF BID BUGTRAQ
matpo -- matpo_link	Cross-site scripting (XSS) vulnerability in view.php in MatPo Link 1.2 Beta allows remote attackers to inject arbitrary web script or HTML via the thema parameter.	2009-04-06	4.3	CVE-2008-6607 BID MILW0RM
michaelfritz -- worldcup typo3 -- typo3	Cross-site scripting (XSS) vulnerability in TARGET-E WorldCup Bets (worldcup) 2.0.0 and earlier extension for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2009-04-10	4.3	CVE-2008-6698 CONFIRM
mit -- kerberos	The get_input_token function in the SPNEGO implementation in MIT Kerberos 5 (aka krb5) 1.5 through 1.6.3 allows remote attackers to cause a denial of service (daemon crash) and possibly obtain sensitive information via a crafted length value that triggers a buffer over-read.	2009-04-08	5.8	CVE-2009-0844 CERT-VN BUGTRAQ CONFIRM
mit -- kerberos	The asn1buf_imbed function in the ASN.1 decoder in MIT Kerberos 5 (aka krb5) 1.6.3, when PK-INIT is used, allows remote attackers to cause a denial of service (application crash) via a crafted length value that triggers an erroneous malloc call, related to incorrect calculations with pointer arithmetic.	2009-04-08	4.3	CVE-2009-0847 BUGTRAQ CONFIRM
mywebland -- minibloggie	del.php in miniBloggie 1.0 allows remote attackers to delete arbitrary posts via a direct request with a modified post_id parameter, a different vulnerability than CVE-2008-4628.	2009-04-07	5.0	CVE-2008-6650 XF BID MILW0RM
opencosmo -- visualsentinel	Cross-site scripting (XSS) vulnerability in Opencosmo VisualSentinel 0.7 allows remote attackers to inject arbitrary web script or HTML via the User-Agent	2009-04-	4.3	CVE-2008-6645

opencosmo -- visualsentinel	header ($_SERVER ['HTTP_USER_AGENT']), which is not properly handled when displaying log files.	07	4.3	BUGTRAQ BUGTRAQ
php -- php	The JSON_parser function (ext/json/JSON_parser.c) in PHP 5.2.x before 5.2.9 allows remote attackers to cause a denial of service (segmentation fault) via a malformed string to the json_decode API function.	2009-04-08	5.0	CVE-2009-1271 CONFIRM MLIST MISC
php -- php	The php_zip_make_relative_path function in php_zip.c in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.	2009-04-08	5.0	CVE-2009-1272 CONFIRM MLIST MISC
quickersite -- quickersite	asp/bs_login.asp in QuickerSite 1.8.5 does not properly restrict access to administrative functionality, which allows remote attackers to (1) change the admin password via the cSaveAdminPW action; (2) modify site information, such as the contact address, via the saveAdmin; and (3) modify the site design via the saveDesign action.	2009-04-08	6.4	CVE-2008-6673 MISC MISC SECUNIA
quickersite -- quickersite	mailPage.asp in QuickerSite 1.8.5 allows remote attackers to flood e-mail accounts with messages via a large number of requests with a modified sEmail parameter.	2009-04-08	5.0	CVE-2008-6674 MISC MISC SECUNIA
quickersite -- quickersite	Multiple cross-site scripting (XSS) vulnerabilities in QuickerSite 1.8.5 allow remote attackers to inject arbitrary web script or HTML via (1) the close parameter to showThumb.aspx; (2) SB_redirect and (3) SB_feedback parameters in process_send.asp, as reachable through default.asp; (4) paramCode and (5) cColor parameters to picker.asp; and the (6) query string, (7) Referer header, and (8) X-FORWARDED-FOR header to rss.asp.	2009-04-08	4.3	CVE-2008-6675 MISC MISC SECUNIA
quickersite -- quickersite	QuickerSite 1.8.5 allows remote attackers to obtain sensitive information via a request to showThumb.aspx without any parameters, which reveals the installation path in an error message.	2009-04-08	5.0	CVE-2008-6676 MISC MISC SECUNIA
resource_library -- tjs_reslib typo3 -- typo3	Cross-site scripting (XSS) vulnerability in Resource Library (tjs_reslib) 0.1.0 and earlier extension for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2009-04-10	4.3	CVE-2008-6699 CONFIRM
simple_machines -- simple_machines_forum	Cross-site request forgery (CSRF) vulnerability in index.php in Simple Machines Forum (SMF) 1.0 before 1.0.15 and 1.1 before 1.1.7 allows remote attackers to hijack the authentication of admins for requests that install packages via the package parameter in an install2 action.	2009-04-07	6.8	CVE-2008-6657 XF CONFIRM BID MILW0RM SECUNIA OSVDB
simple_machines -- simple_machines_forum	Directory traversal vulnerability in index.php in Simple Machines Forum (SMF) 1.0 before 1.0.15 and 1.1 before 1.1.7 allows remote authenticated administrators to install packages from arbitrary directories via a .. (dot dot) in the package parameter during an install2 action, as demonstrated by a predictable package filename in attachments/ that was uploaded through a post2 action to index.php.	2009-04-07	4.0	CVE-2008-6658 CONFIRM MILW0RM OSVDB
simple_machines -- simple_machines_forum	Directory traversal vulnerability in index.php in Simple Machines Forum (SMF) 1.0 before 1.0.15 and 1.1 before 1.1.7 allows remote authenticated users to configure arbitrary local files for execution via directory traversal sequences in the value of the theme_dir field during a jsoption action, related to Sources/QueryString.php and Sources/Themes.php, as demonstrated by a local .gif file in attachments/ with PHP code that was uploaded through a profile2 action to index.php.	2009-04-07	5.5	CVE-2008-6659 CONFIRM BID MILW0RM SECUNIA OSVDB
sitexs_cms -- sitexs_cms	Unrestricted file upload vulnerability in adm/visual/upload.php in SiteXS CMS 0.1.1 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in images/.	2009-04-06	6.8	CVE-2008-6617 XF BID BUGTRAQ

stanislas_rolland -- sr_feuser_register	Frontend User Registration (sr_feuser_register) extension 2.5.20 and earlier for TYPO3 does not properly verify access rights, which allows remote authenticated users to obtain sensitive information such as passwords via unknown attack vectors.	2009-04-07	4.0	CVE-2009-1264 VUPEN BID CONFIRM CONFIRM
structum -- infobiz_server	Cross-site scripting (XSS) vulnerability in search_results.php in InfoBiz Server allows remote attackers to inject arbitrary web script or HTML via the keywords parameter.	2009-04-07	4.3	CVE-2008-6654 XF BID OSVDB SECUNIA MISC
typo3 -- wt_gallery	Directory traversal vulnerability in the wt_gallery extension 2.5.0 and earlier for TYPO3 allows remote attackers to read arbitrary image files and determine directory structure via unspecified vectors.	2009-04-07	5.0	CVE-2008-6630 BID CONFIRM
vertex4 -- sunage	Integer overflow in Vertex4 SunAge 1.08.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted packet to UDP port 27960.	2009-04-08	5.0	CVE-2008-6670 XF VUPEN BID SECUNIA OSVDB MISC MISC
vertex4 -- sunage	Vertex4 SunAge 1.08.1 and earlier allows remote attackers to cause a denial of service ("runtime error") via a crafted join packet to UDP port 27960, probably related to an invalid nickname command.	2009-04-08	5.0	CVE-2008-6672 XF VUPEN BID SECUNIA MISC MISC
vmware -- ace vmware -- player vmware -- server vmware -- workstation	Heap-based buffer overflow in the VNnc Codec in VMware Workstation 6.5.x before 6.5.2 build 156735, VMware Player 2.5.x before 2.5.2 build 156735, VMware ACE 2.5.x before 2.5.2 build 156735, and VMware Server 2.0.x before 2.0.1 build 156745 allows remote attackers to execute arbitrary code via a crafted web page or video file, aka ZDI-CVE-436.	2009-04-06	6.8	CVE-2009-0910 FULLDISC MLIST
webbdomain -- web_shop_online	Cross-site scripting (XSS) vulnerability in detail.php in WEBBDOMAIN Multi Languages WebShop Online 1.02 allows remote attackers to inject arbitrary web script or HTML via the name parameter.	2009-04-06	4.3	CVE-2008-6629 MILW0RM SECUNIA OSVDB
webhelpdesk -- web_help_desk	Multiple cross-site scripting (XSS) vulnerabilities in Web Help Desk 9.1.22 (evaluation version) allow remote attackers to inject arbitrary web script or HTML via the (1) Report Name, (2) Asset No., and (3) Full Name fields in a Models action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-07	4.3	CVE-2009-1261 XF BID SECUNIA
xine -- xine-lib	Integer overflow in the qt_error parse_trak_atom function in demuxers/demux_qt.c in xine-lib 1.1.16.2 and earlier allows remote attackers to execute arbitrary code via a Quicktime movie file with a large count value in an STTS atom, which triggers a heap-based buffer overflow.	2009-04-08	5.0	CVE-2009-1274 XF VUPEN MISC SECTRACK BUGTRAQ CONFIRM SECUNIA OSVDB CONFIRM
yourfreeworld	Cross-site scripting (XSS) vulnerability in listtest.php in Apartment Search Script	2009-04		CVE-2008-6683

yourfreeworld -- apartment_search_script	allows remote attackers to inject arbitrary web script or HTML via the r parameter.	2009-04-10	4.3	XF BID MILW0RM
yourfreeworld -- apartment_search_script	Unrestricted file upload vulnerability in editimage.php in Apartment Search Script allows remote attackers to execute arbitrary code by uploading a file with an executable extension and a GIF header, then accessing this file via a direct request to a renamed file in Member_Admin/logo/.	2009-04-10	6.8	CVE-2008-6684 XF BID MILW0RM
zen-cart -- zen_cart	Cross-site scripting (XSS) vulnerability in index.php in Zen Software Zen Cart 2008 allows remote attackers to inject arbitrary web script or HTML via the keyword parameter in the advanced_search_result page. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-06	4.3	CVE-2008-6616 XF BID MISC

Back to top

Low Vulnerabilities (CVSS Score: 0.0 .. 3.9)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- mod_perl	Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.	2009-04-07	2.6	CVE-2009-0796 CONFIRM
apache -- mod_jk apache -- tomcat	The JK Connector (aka mod_jk) 1.2.0 through 1.2.26 in Apache Tomcat allows remote attackers to obtain sensitive information via an arbitrary request from an HTTP client, in opportunistic circumstances involving (1) a request from a different client that included a Content-Length header but no POST data or (2) a rapid series of requests, related to noncompliance with the AJP protocol's requirements for requests containing Content-Length headers.	2009-04-09	2.6	CVE-2008-5519 CONFIRM BID BUGTRAQ CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM SECTRACK SECUNIA MLIST MLIST
joomla -- joomla	Multiple cross-site scripting (XSS) vulnerabilities in Joomla! 1.5 through 1.5.9 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors to the (1) com_admin component, (2) com_search component when "Gather Search Statistics" is enabled, and (3) the category view in the com_content component.	2009-04-09	2.6	CVE-2009-1279 BID
sun -- opensolaris sun -- solaris	XScreenSaver in Sun Solaris 10 and OpenSolaris before snv_109, and Solaris 8 and 9 with GNOME 2.0 or 2.0.2, allows physically proximate attackers to obtain sensitive information by reading popup windows, which are displayed even when the screen is locked, as demonstrated by Thunderbird new-mail notifications.	2009-04-09	2.1	CVE-2009-1276 SUNALERT CONFIRM

Back to top