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**
adobe -- acrobat adobe -- acrobat_reader adobe -- reader	The getAnnots Doc method in the JavaScript API in Adobe Reader and Acrobat 9.1, 8.1.4, 7.1.1, and earlier allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a PDF file that contains an annotation, and has an OpenAction entry with JavaScript code that calls this method with crafted integer arguments.	2009-04-30	9.3	CVE-2009-1492 XF VUPEN BID SECUNIA MISC CONFIRM MISC
adobe -- flash_media_server	Unspecified vulnerability in Adobe Flash Media Server (FMS) before 3.0.4 and 3.5.x before 3.5.2, as used in Flash Media Interactive Server and Flash Media Streaming Server, allows remote attackers to execute arbitrary remote procedures within an ActionScript file on the server via RPC requests.	2009-05-01	7.5	CVE-2009-1365 BID CONFIRM

bluevirus-design -- sma-db	PHP remote file inclusion vulnerability in format.php in SMA-DB 0.3.12 allows remote attackers to execute arbitrary PHP code via a URL in the _page_content parameter.	2009-04-28	7.5	CVE-2009-1450 MILW0RM
bluevirus-design -- sma-db	Multiple PHP remote file inclusion vulnerabilities in theme/format.php in SMA-DB 0.3.13 allow remote attackers to execute arbitrary PHP code via a URL in the (1) _page_css and (2) _page_javascript parameters. NOTE: the _page_content vector is already is covered by CVE-2009-1450.	2009-04-28	7.5	CVE-2009-1452 XF BID MILW0RM
china-on-site -- flexcustomer0.0.6	Static code injection vulnerability in admin/install.php in Flexcustomer 0.0.6 might allow remote attackers to inject arbitrary PHP code into const.inc.php via the installdbname parameter (aka the Database Name field). NOTE: the installation instructions specify deleting admin/install.php.	2009-04-28	10.0	CVE-2008-6761 XF MILW0RM
cmu -- dbd::pg	Heap-based buffer overflow in the DBD::Pg (aka DBD-Pg or libdbd-pg-perl) module 1.49 for Perl might allow context-dependent attackers to execute arbitrary code via unspecified input to an application that uses the getline and pg_getline functions to read database rows.	2009-04-30	7.5	CVE-2009-0663 CONFIRM
coolplayer -- coolplayer	Stack-based buffer overflow in PortableApps CoolPlayer Portable (aka CoolPlayer+ Portable) 2.19.1 allows remote attackers to execute arbitrary code via a skin file (skin.ini) with a large PlaylistSkin parameter. NOTE: this may overlap CVE-2008-5735.	2009-04-27	9.3	CVE-2009-1449 MILW0RM SECUNIA
drupal -- news_page	SQL injection vulnerability in News Page 5.x before 5.x-1.2 module, a module for Drupal, allows remote attackers, with News Page nodes create and edit privileges, to execute arbitrary SQL commands via the	2009-05-01	7.5	CVE-2009-1505 BID CONFIRM

	Include Words field (keywords parameter).			
drupal -- nodeaccess_userreference	The Node Access User Reference module 5.x before 5.x-2.0-beta4 and 6.x before 6.x-2.0-beta6, a module for Drupal, interprets an empty CCK user reference as a reference to the anonymous user, which might allow remote attackers to bypass intended access restrictions to read or modify a node.	2009-05-01	7.5	CVE-2009-1507 BID CONFIRM
e-cart -- free_shopping_cart	Unrestricted file upload vulnerability in admin/editor/image.php in e-cart.biz Free Shopping Cart 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/.	2009-04-27	7.5	CVE-2009-1447 XF BID MILW0RM SECUNIA
francis_james_franklin -- libwmf	Use-after-free vulnerability in the embedded GD library in libwmf 0.2.8.4 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted WMF file.	2009-05-01	7.5	CVE-2009-1364 CONFIRM CONFIRM BID CONFIRM REDHAT
galaxyscripts -- mini_file_host	Unrestricted file upload vulnerability in Mini File Host 1.5 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 in an unspecified directory, as demonstrated by creating a name.php file.	2009-05-01	7.5	CVE-2008-6785 XF MILW0RM
gomlab -- gom_player	Stack-based buffer overflow in srt2smi.exe in Gretech Online Movie Player (GOM Player) 2.1.16.4635 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long string in an SRT file.	2009-05-01	10.0	CVE-2009-1497 BID BUGTRAQ MILW0RM MISC SECUNIA OSVDB
	Integer overflow in ovalarmsrv.exe in HP OpenView Network Node			CVE-2008

hp -- openview_network_node_manager	Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via a crafted command to TCP port 2954, which triggers a heap-based buffer overflow.	2009-04-28	7.5	CVE-2008-2438 BID HP HP
hypersilence -- silentum_loginsys	login2.php in Silentum LoginSys 1.0.0 allows remote attackers to bypass authentication and obtain access to an arbitrary account by setting the logged_in cookie to that account's username.	2009-04-28	7.5	CVE-2008-6763 XF BID OSVDB MILW0RM SECUNIA
ivano_culmine -- webportal_cms	Multiple directory traversal vulnerabilities in WebPortal CMS 0.8-beta allow remote attackers to (1) read arbitrary files via directory traversal sequences in the lang parameter to libraries/helpdocs/help.php and (2) include and execute arbitrary local files via directory traversal sequences in the error parameter to index.php.	2009-04-27	7.5	CVE-2009-1445 BID MILW0RM
jeremy_powers -- lizardware_cms	SQL injection vulnerability in administrator/index.php in Lizardware CMS 0.6.0 and earlier allows remote attackers to execute arbitrary SQL commands via the user.	2009-05-01	10.0	CVE-2008-6787 XF BID MILW0RM
joomla -- com_mailto	SQL injection vulnerability in the MailTo (aka com_mailto) component in Joomla! allows remote attackers to execute arbitrary SQL commands via the article parameter in index.php. NOTE: SecurityFocus states that this issue has been disputed by the vendor.	2009-05-01	7.5	CVE-2009-1499 BID MILW0RM
keir_davis -- x-forum	SQL injection vulnerability in the xforum_validateUser function in Common.php in X-Forum 0.6.2 allows remote attackers to execute arbitrary SQL commands, as demonstrated via the cookie_username parameter to Configure.php.	2009-05-01	7.5	CVE-2009-1508 XF BID MILW0RM

konstanty_bialkowski -- libmodplug	Integer overflow in the CSoundFile::ReadMed function (src/load_med.cpp) in libmodplug before 0.8.6, as used in gstreamer-plugins and other products, allows context-dependent attackers to execute arbitrary code via a MED file with a crafted (1) song comment or (2) song name, which triggers a heap-based buffer overflow.	2009-04-27	7.5	CVE-2009-1438 VUPEN BID CONFIRM OSVDB
linux -- kernel	Buffer overflow in fs/cifs/connect.c in CIFS in the Linux kernel 2.6.29 and earlier allows remote attackers to cause a denial of service (crash) via a long nativeFileSystem field in a Tree Connect response to an SMB mount request.	2009-04-27	7.8	CVE-2009-1439 CONFIRM MLIST MLIST MLIST MLIST MISC
matteoiammarrone -- s-cms	Directory traversal vulnerability in plugin.php in S-Cms 1.1 Stable and 1.5.2 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the page parameter.	2009-05-01	7.5	CVE-2009-1502 BID MILW0RM SECUNIA
microsoft -- windows	GDI+ in Microsoft Windows XP SP3 allows remote attackers to cause a denial of service (infinite loop) via a PNG file that contains a certain large btChunkLen value.	2009-05-01	7.8	CVE-2009-1511 BID MILW0RM
myiosoft -- ajaxportal	SQL injection vulnerability in ajaxp_backend.php in MyioSoft AjaxPortal 3.0 allows remote attackers to execute arbitrary SQL commands via the page parameter.	2009-05-01	7.5	CVE-2009-1509 BID MILW0RM SECUNIA
ninjadesigns -- flatchat	Directory traversal vulnerability in pmscript.php in Flatchat 3.0 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the with parameter.	2009-04-29	7.5	CVE-2009-1486 MILW0RM
ocsinventory-ng -- ocs_inventory_ng	Multiple unspecified vulnerabilities in the Server component in OCS Inventory NG before 1.02 have unknown impact and attack vectors.	2009-04-27	10.0	CVE-2009-1443 CONFIRM
	login/register_form.php in YourPlace 1.0.2 and earlier does not check that a			CVE-2008-

peterselie -- yourplace	username already exists when a new account is created, which allows remote attackers to bypass intended access restrictions by registering a new account with the username of a target user.	2009-04-29	7.5	6772 XF BID MILW0RM SECUNIA
pjhome -- puterjams_blog	SQL injection vulnerability in action.asp in PuterJam's Blog (PJBlog3) 3.0.6.170 allows remote attackers to execute arbitrary SQL commands via the cname parameter in a checkAlias action, as exploited in the wild in April 2009. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-29	7.5	CVE-2009-1481 XF BID SECUNIA OSVDB MISC
razorcms -- razorcms	The Security Manager in razorCMS before 0.4 does not verify the permissions of every file owned by the apache user account, which is inconsistent with the documentation and allows local users to have an unspecified impact.	2009-04-28	7.2	CVE-2009-1462 BID CONFIRM FULLDISC FULLDISC
razorcms -- razorcms	Static code injection vulnerability in razorCMS before 0.4 allows remote attackers to inject arbitrary PHP code into any page by saving content as a .php file.	2009-04-28	7.5	CVE-2009-1463 BID CONFIRM FULLDISC FULLDISC
rens_rikkerink -- fungamez	SQL injection vulnerability in pages/login.php in FunGamez RC1 allows remote attackers to execute arbitrary SQL commands via the login_user (aka username) parameter. NOTE: some of these details are obtained from third party information.	2009-04-29	7.5	CVE-2009-1487 XF VUPEN BID MILW0RM BUGTRAQ
rens_rikkerink -- fungamez	includes/user.php in Fungamez RC1 allows remote attackers to bypass authentication and gain administrative access by setting the user cookie parameter.	2009-04-29	7.5	CVE-2009-1489 VUPEN MILW0RM BUGTRAQ
sahil_ahuja -- pragyan_cms	SQL injection vulnerability in index.php Pragyan CMS 2.6.4 allows remote attackers to execute arbitrary	2009-04-	7.5	CVE-2009-1480 BID

sahil_ahuja -- pragyan_cms	SQL commands via the fileget parameter in a view action and other unspecified vectors.	29	7.5	BID BUGTRAQ MILW0RM
sarkilar -- sarkilar	SQL injection vulnerability in the Sarkilar module for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the id parameter in a showcontent action to modules.php.	2009-05-01	7.5	CVE-2008-6779 XF BID MISC
scripts-for-sites -- ez_hot_or_not	SQL injection vulnerability in viewcomments.php in Scripts For Sites (SFS) EZ Hot or Not allows remote attackers to execute arbitrary SQL commands via the phid parameter.	2009-05-01	7.5	CVE-2008-6776 XF MILW0RM SECUNIA OSVDB
scripts-for-sites -- ez_auction	SQL injection vulnerability in viewfaqs.php in Scripts for Sites (SFS) EZ Auction allows remote attackers to execute arbitrary SQL commands via the cat parameter.	2009-05-01	7.5	CVE-2008-6778 XF BID MILW0RM SECUNIA OSVDB
scripts-for-sites -- ez_affiliate	SQL injection vulnerability in directory.php in Scripts for Sites (SFS) SFS EZ Affiliate allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a list action.	2009-05-01	7.5	CVE-2008-6780 MILW0RM SECUNIA OSVDB
scripts-for-sites -- ez_gaming_directory	SQL injection vulnerability in directory.php in Sites for Scripts (SFS) Gaming Directory allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a list action.	2009-05-01	7.5	CVE-2008-6781 XF BID MILW0RM SECUNIA OSVDB
scripts-for-sites -- ez_hosting_directory	SQL injection vulnerability in directory.php in Sites for Scripts (SFS) EZ Hosting Directory allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a list action.	2009-05-01	7.5	CVE-2008-6782 XF BID OSVDB MILW0RM SECUNIA
	SQL injection vulnerability in directory.php in Sites for Scripts			CVE-2008-6783 XF

scripts-for-sites -- ez_home_business_directory	(SFS) EZ Home Business Directory allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a list action.	2009-05-01	7.5	XF BID OSVDB MILW0RM SECUNIA
scripts-for-sites -- ez_adult_directory	SQL injection vulnerability in directory.php in Scripts For Sites (SFS) EZ Adult Directory allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a list action.	2009-05-01	7.5	CVE-2008-6784 XF BID OSVDB MILW0RM SECUNIA
symantec -- brightmail_gateway_appliance	Multiple unspecified vulnerabilities in the Control Center in Symantec Brightmail Gateway Appliance before 8.0.1 allow remote authenticated users to gain privileges, and possibly obtain sensitive information or hijack sessions of arbitrary users, via vectors involving (1) administrative scripts or (2) console functions.	2009-04-24	9.0	CVE-2009-0064 VUPEN CONFIRM SECTRACK
symantec -- antivirus symantec -- antivirus_central_quarantine_server symantec -- client_security symantec -- endpoint_protection symantec -- system_center	The Intel LANDesk Common Base Agent (CBA) in Symantec Alert Management System 2 (AMS2), as used in Symantec System Center (SSS); Symantec AntiVirus Server; Symantec AntiVirus Central Quarantine Server; Symantec AntiVirus (SAV) Corporate Edition 9 before 9.0 MR7, 10.0 and 10.1 before 10.1 MR8, and 10.2 before 10.2 MR2; Symantec Client Security (SCS) 2 before 2.0 MR7 and 3 before 3.1 MR8; and Symantec Endpoint Protection (SEP) before 11.0 MR3, allows remote attackers to execute arbitrary commands via a crafted packet whose contents are interpreted as a command to be launched in a new process.	2009-04-29	10.0	CVE-2009-1429 CONFIRM BID
	Multiple stack-based buffer overflows in IAO.EXE in the Intel Alert Originator Service in Symantec Alert Management System 2 (AMS2), as used in Symantec System Center (SSS); Symantec			

symantec -- antivirus symantec -- antivirus_central_quarantine_server symantec -- client_security symantec -- endpoint_protection symantec -- system_center	AntiVirus Server; Symantec AntiVirus Central Quarantine Server; Symantec AntiVirus (SAV) Corporate Edition 9 before 9.0 MR7, 10.0 and 10.1 before 10.1 MR8, and 10.2 before 10.2 MR2; Symantec Client Security (SCS) 2 before 2.0 MR7 and 3 before 3.1 MR8; and Symantec Endpoint Protection (SEP) before 11.0 MR3, allow remote attackers to execute arbitrary code via (1) a crafted packet or (2) data that ostensibly arrives from the MsgSys.exe process.	2009-04-29	9.3	CVE-2009-1430 MISC CONFIRM BID BID
symantec -- antivirus symantec -- antivirus_central_quarantine_server symantec -- client_security symantec -- endpoint_protection symantec -- system_center	XFR.EXE in the Intel File Transfer service in the console in Symantec Alert Management System 2 (AMS2), as used in Symantec System Center (SSS); Symantec AntiVirus Server; Symantec AntiVirus Central Quarantine Server; Symantec AntiVirus (SAV) Corporate Edition 9 before 9.0 MR7, 10.0 and 10.1 before 10.1 MR8, and 10.2 before 10.2 MR2; Symantec Client Security (SCS) 2 before 2.0 MR7 and 3 before 3.1 MR8; and Symantec Endpoint Protection (SEP) before 11.0 MR3, allows remote attackers to execute arbitrary code by placing the code on a (1) share or (2) WebDAV server, and then sending the UNC share pathname to this service.	2009-04-29	9.3	CVE-2009-1431 CONFIRM BID IDEFENSE
tibco -- enterprise_message_service tibco -- rtworks tibco -- smartsockets_rtserver	Stack-based buffer overflow in TIBCO SmartSockets before 6.8.2, SmartSockets Product Family (aka RTworks) before 4.0.5, and Enterprise Message Service (EMS) 4.0.0 through 5.1.1, as used in SmartSockets Server and RTworks Server (aka RTserver), SmartSockets client libraries and add-on products, RTworks libraries and components, EMS Server (aka tibemsd), SmartMQ, iProcess Engine,	2009-04-30	10.0	CVE-2009-1291 CONFIRM CONFIRM

	ActiveMatrix products, and CA Enterprise Communicator, allows remote attackers to execute arbitrary code via "inbound data," as demonstrated by requests to the UDP interface of the RTserver component, and data injection into the TCP stream to tibemsd.			CONFIRM
tigerdms -- tigerdms	Multiple SQL injection vulnerabilities in login.php in Tiger Document Management System (DMS) allow remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters.	2009-05-01	7.5	CVE-2009-1503 MILW0RM SECUNIA
webportal -- webportal_cms	PHP remote file inclusion vulnerability in indexk.php in WebPortal CMS 0.8-beta allows remote attackers to execute arbitrary PHP code via a URL in the lib_path parameter.	2009-04-27	7.5	CVE-2009-1444 BID MILW0RM
wordpress -- wordpress	wp-admin/upgrade.php in WordPress, probably 2.6.x, allows remote attackers to upgrade the application, and possibly cause a denial of service (application outage), via a direct request.	2009-04-28	10.0	CVE-2008-6767 BUGTRAQ
xigla -- absolute_control_panel_xe	Absolute Form Processor XE 1.5 allows remote attackers to bypass authentication and gain administrative access by setting the xlaAFPadmin cookie to "lvl=1&userid=1."	2009-05-01	7.5	CVE-2009-1504 MILW0RM

Back to top

Medium Vulnerabilities (CVSS Score: 4.0 .. 6.9)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat adobe -- acrobat_reader adobe -- reader	The customDictionaryOpen spell method in the JavaScript API in Adobe Reader 8.1.4 and 9.1 on Linux allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a PDF file that triggers a call to this method with a long string in the	2009-04-30	6.8	CVE-2009-1493 MISC

	second argument.			
aemuleplus -- emule_plus emuleplus -- emule_plus	The logging feature in eMule Plus before 1.2e allows remote attackers to cause a denial of service (infinite loop) via unspecified attack vectors.	2009-04-29	5.0	CVE-2009-1485 XF CONFIRM SECUNIA
amule -- amule	Incomplete blacklist vulnerability in DownloadListCtrl.cpp in amule 2.2.4 allows remote attackers to conduct argument injection attacks into a command for mplayer via a crafted filename.	2009-04-27	6.8	CVE-2009-1440 MLIST MISC
andrew_simpson -- webcollab	Cross-site scripting (XSS) vulnerability in tasks.php in WebCollab before 2.50 (aka Billy Goat) allows remote attackers to inject arbitrary web script or HTML via the selection parameter in a todo action.	2009-04-28	4.3	CVE-2009-1454 CONFIRM MISC
andrew_simpson -- webcollab	Multiple cross-site request forgery (CSRF) vulnerabilities in WebCollab before 2.50 (aka Billy Goat) allow remote attackers to hijack the authentication of administrators for requests that change an arbitrary password or have other unspecified impact.	2009-04-28	6.8	CVE-2009-1455 CONFIRM MISC
anoochit_chalothorn -- tiny_blogr	SQL injection vulnerability in class.eport.php in Tiny Blogr 1.0.0 rc4, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the txtUsername parameter (aka the Username field). NOTE: some of these details are obtained from third party information.	2009-04-28	6.8	CVE-2009-1453 BID BUGTRAQ MILW0RM SECUNIA
apple -- cups	The web interface for CUPS before 1.3.10 does not validate the HTTP Host header in a client request, which makes it easier for remote attackers to conduct DNS rebinding attacks.	2009-04-24	6.4	CVE-2009-0164 CONFIRM CONFIRM CONFIRM
bernie_innocenti -- geeki_geeki	Multiple directory traversal vulnerabilities in geekigeeki.py in GeekiGeeki before 3.0 allow remote attackers to read arbitrary files via directory traversal sequences in a pagename argument in the (1) handle_edit and (2) handle_raw functions.	2009-05-01	5.0	CVE-2008-6786 OSVDB
	Cross-site scripting (XSS) vulnerability in			CVE-2009

bluevirus-design -- sma-db	startpage.php in SMA-DB 0.3.12 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2009-04-28	4.3	CVE-2009-1451 MILW0RM
debian -- libdbd-pg-perl debiandbd-pg-perl -- 0.94 debianl -- libdbd-pg-perl ldebian -- libdbd-pg-perl	Memory leak in the dequote_bytea function in quote.c in the DBD::Pg (aka DBD-Pg or libdbd-pg-perl) module before 2.0.0 for Perl allows context-dependent attackers to cause a denial of service (memory consumption) by fetching data with BYTEA columns.	2009-04-30	5.0	CVE-2009-1341 MISC DEBIAN CONFIRM CONFIRM CONFIRM
elkagroup -- image_gallery	Unrestricted file upload vulnerability in upload.php in Elkagroup Image Gallery 1.0 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in gallery/pictures/. NOTE: some of these details are obtained from third party information.	2009-04-27	6.5	CVE-2009-1446 VUPEN BID MILW0RM SECUNIA
evolution-extreme -- nuke_evolution_xtreme	Cross-site scripting (XSS) vulnerability in player.php in Nuke Evolution Xtreme 2.x allows remote attackers to inject arbitrary web script or HTML via the defaultVisualExt parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-28	4.3	CVE-2009-1457 XF BID SECUNIA OSVDB
exif -- exif	Cross-site scripting (XSS) vulnerability in the Exif module 5.x-1.x before 5.x-1.2 and 6.x-1.x-dev before April 13, 2009, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via EXIF tags in an image.	2009-05-01	4.3	CVE-2009-1501 BID CONFIRM
foswiki -- foswiki	Cross-site request forgery (CSRF) vulnerability in Foswiki before 1.0.5 allows remote attackers to hijack the authentication of arbitrary users for requests that modify pages, change permissions, or change group memberships, as demonstrated by a URL for a (1) save or (2) view script in the SRC attribute of an IMG element, a related issue to CVE-2009-1339.	2009-04-30	6.8	CVE-2009-1434 MLIST CONFIRM
	The db interface in libc in FreeBSD 6.3, 6.4, 7.0, 7.1, and 7.2-PRERELEASE does			

freebsd -- freebsd	not properly initialize memory for Berkeley DB 1.85 database structures, which allows local users to obtain sensitive information by reading a database file.	2009-04-27	4.9	CVE-2009-1436 BID
gecad -- axigen_mail_server	Cross-site scripting (XSS) vulnerability in the web mail interface feature in AXIGEN Mail Server 6.2.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving e-mail messages. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-29	4.3	CVE-2009-1484 BID SECUNIA
gnu -- gnutls	lib/pk-libgcrypt.c in libgnutls in GnuTLS before 2.6.6 does not properly handle invalid DSA signatures, which allows remote attackers to cause a denial of service (application crash) and possibly have unspecified other impact via a malformed DSA key that triggers a (1) free of an uninitialized pointer or (2) double free.	2009-04-30	4.3	CVE-2009-1415 MLIST
gnu -- gnutls	lib/gnutls_pk.c in libgnutls in GnuTLS 2.5.0 through 2.6.5 generates RSA keys stored in DSA structures, instead of the intended DSA keys, which might allow remote attackers to spoof signatures on certificates or have unspecified other impact by leveraging an invalid DSA key.	2009-04-30	6.0	CVE-2009-1416 MLIST
gnu -- gnutls	gnutls-cli in GnuTLS before 2.6.6 does not verify the activation and expiration times of X.509 certificates, which allows remote attackers to successfully present a certificate that is (1) not yet valid or (2) no longer valid, related to lack of time checks in the _gnutls_x509_verify_certificate function in lib/x509/verify.c in libgnutls_x509, as used by (a) Exim, (b) OpenLDAP, and (c) libsoup.	2009-04-30	5.0	CVE-2009-1417 MLIST
hp -- hp-ux	Unspecified vulnerability in useradd in HP HP-UX B.11.11, B.11.23, and B.11.31 allows local users to access arbitrary files and directories via	2009-04-29	6.0	CVE-2009-0719 BID

	unknown vectors, a different issue than CVE-2008-1660.			BID
hypersilence -- silentum_loginsys	Cross-site scripting (XSS) vulnerability in login.php in Silentum LoginSys 1.0.0 allows remote attackers to inject arbitrary web script or HTML via the message parameter.	2009-04-28	4.3	CVE-2008-6764 XF BID OSVDB SECUNIA MISC
idb -- idb	Directory traversal vulnerability in inc/profilemain.php in Game Maker 2k Internet Discussion Boards (iDB) 0.2.5 Pre-Alpha SVN 243 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the skin parameter in a settings action to profile.php.	2009-05-01	6.8	CVE-2009-1498 XF BID MILW0RM
intelliants -- elitius	SQL injection vulnerability in classes/Xp.php in eLitius 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter to banner-details.php.	2009-05-01	6.5	CVE-2009-1506 BID MILW0RM
joomla -- cmimarketplace	Directory traversal vulnerability in the Cmi Marketplace (com_cmimarketplace) component 0.1 for Joomla! allows remote attackers to list arbitrary directories via a .. (dot dot) in the viewit parameter to index.php.	2009-05-01	5.0	CVE-2009-1496 BID MILW0RM
keir_davis -- x-forum	Static code injection vulnerability in X-Forum 0.6.2 allows remote authenticated administrators to inject arbitrary PHP code into Config.php via the adminEMail parameter to SaveConfig.php.	2009-05-01	6.5	CVE-2009-1512 MILW0RM
koschtit -- koschtit_image_gallery	Multiple directory traversal vulnerabilities in KoschtIT Image Gallery 1.82 allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the file parameter to (1) ki_makepic.php and (2) ki_nojsdisplayimage.php in ki_base/.	2009-05-01	6.4	CVE-2009-1510 BID MILW0RM
lovpop -- apricot	Cross-site scripting (XSS) vulnerability in apricot.php in LovPop.net APRICOT, probably 1.20, allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2009-04-27	4.3	CVE-2009-1448 XF JVNDB JVN

memcachedb -- memcached	The process_stat function in (1) Memcached before 1.2.8 and (2) MemcacheDB 1.2.0 discloses (a) the contents of /proc/self/maps in response to a stats maps command and (b) memory-allocation statistics in response to a stats malloc command, which allows remote attackers to obtain sensitive information such as the locations of memory regions, and defeat ASLR protection, by sending a command to the daemon's TCP port.	2009-04-30	5.0	CVE-2009-1255 CONFIRM
memcachedb -- memcached	The process_stat function in Memcached 1.2.8 discloses memory-allocation statistics in response to a stats malloc command, which allows remote attackers to obtain potentially sensitive information by sending this command to the daemon's TCP port.	2009-04-30	5.0	CVE-2009-1494 MISC MISC MISC
mephisteus -- the_personal_sticky_threads	The Personal Sticky Threads addon 1.0.3c for vBulletin allows remote authenticated users to read the title, author, and pages of an arbitrary thread by toggling a personal sticky.	2009-04-27	4.0	CVE-2008-6754 BID BUGTRAQ SECUNIA OSVDB
moinmo -- moinmoin moinmoin -- moinmoin	Multiple cross-site scripting (XSS) vulnerabilities in action/AttachFile.py in MoinMoin 1.8.2 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) an AttachFile sub-action in the error_msg function or (2) multiple vectors related to package file errors in the upload_form function, different vectors than CVE-2009-0260.	2009-04-29	4.3	CVE-2009-1482 CONFIRM
mozilla -- firefox	The nsTextFrame::ClearTextRun function in layout/generic/nsTextFrameThebes.cpp in Mozilla Firefox 3.0.9 allows remote attackers to cause a denial of service (memory corruption) and probably execute arbitrary code via unspecified vectors. NOTE: this vulnerability reportedly exists because of an incorrect fix for CVE-2009-1302.	2009-04-30	6.8	CVE-2009-1313 REDHAT CONFIRM CONFIRM CONFIRM CONFIRM BID CONFIRM SECTRACK SECTRACK
				CVE-2008-

mseclab -- htc_touch_cruise mseclab -- htc_touch_pro	HTC Touch Pro and HTC Touch Cruise vCard allows remote attackers to cause denial of service (CPU consumption, SMS consumption, and connectivity loss) via a flood of vCards to UDP port 9204.	2009-05-01	5.0	6775 XF BUGTRAQ MISC OSVDB FULLDISC
myphp -- myphp_forum	Multiple SQL injection vulnerabilities in MyPHP Forum 3.0 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) id parameter in a confirm action, the (2) user parameter in a newconfirm action, and (3) reqpwd action to member.php; and the (4) quote parameter in a post action and (5) pid parameter in an edit action to post.php, different vectors than CVE-2005-0413.2 and CVE-2007-6667.	2009-05-01	6.0	CVE-2008-6777 XF BID MILW0RM SECUNIA
peterselie -- yourplace	Unrestricted file upload vulnerability in upload.php in YourPlace 1.0.2 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file.	2009-04-29	6.0	CVE-2008-6769 XF BID MILW0RM
peterselie -- yourplace	YourPlace 1.0.2 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to a database containing user credentials via a direct request for users.txt.	2009-04-29	5.0	CVE-2008-6770 XF BID MILW0RM SECUNIA
peterselie -- yourplace	YourPlace 1.0.2 and earlier allows remote attackers to obtain sensitive system information via a direct request via a direct request to user/uploads/phpinfo.php, which calls the phpinfo function.	2009-04-29	5.0	CVE-2008-6771 XF BID MILW0RM SECUNIA
peterselie -- yourplace	Static code injection vulnerability in user/internettoolbar/edit.php in YourPlace 1.0.2 and earlier allows remote authenticated users to execute arbitrary PHP code into user/internettoolbar/index.php via the (1) fav1_url, (2) fav1_name, (3) fav2_url, (4) fav2_name, (5) fav3_url, (6) fav3_name, (7) fav4_url, (8) fav4_name, (9) fav5_url, or (10) fav5_name parameters.	2009-04-29	6.5	CVE-2008-6773 XF BID MILW0RM SECUNIA

peterselie -- yourplace	internettoolbar/edit.php in YourPlace 1.0.2 and earlier does not end execution when an invalid username is detected, which allows remote attackers to bypass intended restrictions and edit toolbar settings via an invalid username. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-29	5.0	CVE-2008-6774 XF SECUNIA
projectcms -- projectcms	SQL injection vulnerability in index.php in ProjectCMS 1.0 Beta allows remote attackers to execute arbitrary SQL commands via the sn parameter.	2009-05-01	6.8	CVE-2009-1500 BID MILW0RM
razorcms -- razorcms	Multiple cross-site scripting (XSS) vulnerabilities in admin/index.php in razorCMS before 0.4 allow remote attackers to inject arbitrary web script or HTML via (1) the slab parameter in an edit action, (2) the catname parameter in a showcats action, and (3) the cat parameter in a reordercat action.	2009-04-28	4.3	CVE-2009-1458 XF BID SECUNIA CONFIRM OSVDB FULLDISC FULLDISC
razorcms -- razorcms	Cross-site request forgery (CSRF) vulnerability in razorCMS before 0.4 allows remote attackers to hijack the authentication of administrators for requests that create a web page containing PHP code.	2009-04-28	6.8	CVE-2009-1459 XF BID SECUNIA CONFIRM OSVDB FULLDISC FULLDISC
razorcms -- razorcms	razorCMS before 0.4 uses weak permissions for (1) admin/core/admin_config.php, which allows local users to obtain the administrator's password hash and FTP user credentials; and (2) the root directory, (3) datastore/, and (4) admin/core/, which allows local users to have an unspecified impact.	2009-04-28	4.6	CVE-2009-1460 XF BID SECUNIA CONFIRM OSVDB FULLDISC FULLDISC
rens_rikkerink -- fungamez	Directory traversal vulnerability in admin/load.php in FunGamez RC1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the	2009-04-29	6.8	CVE-2009-1488 XF VUPEN BID

	module parameter to index.php.			MILW0RM BUGTRAQ
shopsystem-forum -- k&s_shopsoftware	Unrestricted file upload vulnerability in admin/editor/images.php in K&S Shopsoftware allows remote attackers to execute arbitrary PHP code by uploading a file with an executable extension, then accessing it via a direct request to the file in images/upload/.	2009-04-29	6.8	CVE-2008-6768 XF BID MILW0RM SECUNIA
stephane_rajalu -- malleo	Directory traversal vulnerability in admin.php in Malleo 1.2.3 allows remote authenticated administrators to include and execute arbitrary local files via a .. (dot dot) in the module parameter.	2009-04-28	6.0	CVE-2009-1456 BID BUGTRAQ SECUNIA
studiolounge -- address_book	Unrestricted file upload vulnerability in upload-file.php in Adam Patterson Studio Lounge Address Book 2.5, as reachable from index2.php, 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 profiles/.	2009-04-29	6.8	CVE-2009-1483 XF VUPEN BID OSVDB MILW0RM SECUNIA
sun -- jdk	Algorithmic complexity vulnerability in the java.util.regex.Pattern.compile method in Sun Java Development Kit (JDK) before 1.6, when used with spring.jar in SpringSource Spring Framework 1.1.0 through 2.5.6 and 3.0.0.M1 through 3.0.0.M2 and dm Server 1.0.0 through 1.0.2, allows remote attackers to cause a denial of service (CPU consumption) via serializable data with a long regex string containing multiple optional groups, a related issue to CVE-2004-2540.	2009-04-27	5.0	CVE-2009-1190 CONFIRM XF CONFIRM BUGTRAQ MISC SECUNIA
sun -- opensolaris sun -- solaris	Multiple unspecified vulnerabilities in the DTrace ioctl handlers in Sun Solaris 10, and OpenSolaris before snv_114, allow local users to cause a denial of service (panic) via unknown vectors.	2009-04-29	4.9	CVE-2009-1478 SUNALERT
symantec -- brightmail_gateway_appliance	Cross-site scripting (XSS) vulnerability in the Control Center in Symantec Brightmail Gateway Appliance before 8.0.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2009-04-24	4.3	CVE-2009-0063 VUPEN CONFIRM SECTRACK

symantec -- antivirus symantec -- endpoint_protection symantec -- norton_360 symantec -- norton_internet_security	Multiple cross-site scripting (XSS) vulnerabilities in ccLgView.exe in the Symantec Log Viewer, as used in Symantec AntiVirus (SAV) before 10.1 MR8, Symantec Endpoint Protection (SEP) 11.0 before 11.0 MR1, Norton 360 1.0, and Norton Internet Security 2005 through 2008, allow remote attackers to inject arbitrary web script or HTML via a crafted e-mail message, related to "two parsing errors."	2009-04-29	4.3	CVE-2009-1428 CONFIRM
symantec -- antivirus symantec -- client_security symantec -- endpoint_protection symantec -- endpoint_protection_protection	Symantec Reporting Server, as used in Symantec AntiVirus (SAV) Corporate Edition 10.1 before 10.1 MR8 and 10.2 before 10.2 MR2, Symantec Client Security (SCS) before 3.1 MR8, and the Symantec Endpoint Protection Manager (SEPM) component in Symantec Endpoint Protection (SEP) before 11.0 MR2, allows remote attackers to inject arbitrary text into the login screen, and possibly conduct phishing attacks, via vectors involving a URL that is not properly handled.	2009-04-30	5.0	CVE-2009-1432 XF VUPEN CONFIRM BID SECTRACK SECTRACK SECTRACK SECUNIA
tim_hockin -- acpid	The daemon in acpid before 1.0.10 allows remote attackers to cause a denial of service (CPU consumption and connectivity loss) by opening a large number of UNIX sockets without closing them, which triggers an infinite loop.	2009-04-24	5.0	CVE-2009-0798 CONFIRM
twiki -- twiki	Cross-site request forgery (CSRF) vulnerability in TWiki before 4.3.1 allows remote authenticated users to hijack the authentication of arbitrary users for requests that update pages, as demonstrated by a URL for a save script in the SRC attribute of an IMG element, a related issue to CVE-2009-1434.	2009-04-30	6.0	CVE-2009-1339 SECTRACK
viart -- viart_shop	Cross-site scripting (XSS) vulnerability in manuals_search.php in ViArt Shop (aka Shopping Cart) 3.5 allows remote attackers to inject arbitrary web script or HTML via the manuals_search parameter.	2009-04-28	4.3	CVE-2008-6757 SECTRACK BID BUGTRAQ OSVDB SECUNIA

viart -- viart_shop	Cross-site request forgery (CSRF) vulnerability in cart_save.php in ViArt Shop (aka Shopping Cart) 3.5 allows remote attackers to hijack the authentication of arbitrary users for requests that conduct persistent cross-site scripting (XSS) attacks via the cart_name parameter in a save action.	2009-04-28	6.8	CVE-2008-6758 SECTRACK BID BUGTRAQ SECUNIA OSVDB OSVDB
viart -- viart_shop	ViArt Shop (aka Shopping Cart) 3.5 allows remote attackers to obtain sensitive information via a URL in the POST_DATA parameter to manuals_search.php, which reveals the installation path in an error message.	2009-04-28	4.3	CVE-2008-6759 SECTRACK BID BUGTRAQ OSVDB
viart -- viart_shop	ViArt Shop (aka Shopping Cart) 3.5 allows remote attackers to obtain sensitive information via an unauthenticated add and save action for a shopping cart in cart_save.php, which reveals the SQL table names in an error message, related to code that mishandles the lack of a user_id parameter.	2009-04-28	4.3	CVE-2008-6760 SECTRACK BID BUGTRAQ OSVDB
viart -- viart_shop	ViArt Shop (aka Shopping Cart) 3.5 allows remote attackers to access the contents of an arbitrary shopping cart via a modified cart_name parameter.	2009-04-28	4.3	CVE-2008-6765 SECTRACK BID BUGTRAQ
viart -- viart_shop	cart_save.php in ViArt Shop (aka Shopping Cart) 3.5 allows remote attackers to cause a denial of service (excessive shopping carts) via a flood of requests.	2009-04-28	4.3	CVE-2008-6766 SECTRACK BUGTRAQ OSVDB
webfileexplorer -- web_file_explorer	Web File Explorer 3.1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for data/db.mdb.	2009-05-01	5.0	CVE-2009-1495 MILW0RM SECUNIA
wordpress -- wordpress	Open redirect vulnerability in wp-admin/upgrade.php in WordPress, probably 2.6.x, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the backto parameter.	2009-04-28	4.3	CVE-2008-6762 OSVDB BUGTRAQ
	ZoneMinder 1.23.3 on Fedora 10 sets the ownership of /etc/zm.conf to the apache			CVE-2008

zoneminder -- zoneminder	user account, and sets the permissions to 0600, which makes it easier for remote attackers to modify this file by accessing it through a (1) PHP or (2) CGI script.	2009-04-27	5.0	CVE-2008-6755 FEDORA

Back to top

Low Vulnerabilities (CVSS Score: 0.0 .. 3.9)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apport -- apport ubuntu -- ubuntu	Apport before 0.108.4 on Ubuntu 8.04 LTS, before 0.119.2 on Ubuntu 8.10, and before 1.0-0ubuntu5.2 on Ubuntu 9.04 does not properly remove files from the application's crash-report directory, which allows local users to delete arbitrary files via unspecified vectors.	2009-04-30	1.9	CVE-2009-1295 CONFIRM MISC UBUNTU BID
mcafee -- active_virus_defense mcafee -- active_virusscan mcafee -- email_gateway mcafee -- internet_security_suite mcafee -- security_for_email_servers mcafee -- security_for_microsoft_sharepoint mcafee -- security_shield mcafee -- total_protection mcafee -- total_protection_for_endpoint mcafee -- virusscan mcafee -- virusscan_commandline mcafee -- virusscan_enterprise	The AV engine before DAT 5600 in McAfee VirusScan, Total Protection, Internet Security, SecurityShield for Microsoft ISA Server, Security for Microsoft Sharepoint, Security for Email Servers, Email Gateway, and Active Virus Defense allows remote attackers to bypass virus detection via (1) an invalid Headflags field in a malformed RAR archive, (2) an invalid Packsize field in a malformed RAR archive, or (3) an invalid Filelength field in a malformed ZIP archive.	2009-04-30	0.0	CVE-2009-1348 CONFIRM
razorcms -- razorcms	Cross-site scripting (XSS) vulnerability in the Create New Page form in razorCMS 0.3 RC2 and earlier allows remote authenticated users to inject arbitrary web script or HTML via the Page Title field.	2009-04-28	3.5	CVE-2009-1461 MISC FULLDISC
trendmicro -- officescan	NTRtScan.exe in Trend Micro OfficeScan Client 8.0 SP1 and 8.0 SP1 Patch 1 allows local users to cause a denial of service (application crash) via directories with long pathnames.	2009-04-27	2.1	CVE-2009-1435 VUPEN SECTRACK BID BUGTRAQ

	NOTE: some of these details are obtained from third party information.			BUGTRAQ SECUNIA OSVDB MISC
zoneminder -- zoneminder	ZoneMinder 1.23.3 on Gentoo Linux uses 0644 permissions for /etc/zm.conf, which allows local users to obtain the database username and password by reading this file.	2009-04-27	2.1	CVE-2008-6756 CONFIRM

Back to top