Please note that US-CERT has changed the look and scope of the Cyber Security Bulletin.

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
AlstraSoft -- Article Manager Pro	SQL injection vulnerability in Alstrasoft Article Manager Pro 1.6 allows remote attackers to execute arbitrary SQL commands via (1) the author_id parameter in profile.php and (2) the aut_id parameter in userarticles.php. NOTE: the aut_id vector can produce resultant path disclosure if the SQL manipulation is invalid.	unknown 2006-05-24	7.0	CVE-2006-2565 BUGTRAQ FRSIRT SECUNIA
BoastMachine -- BoastMachine Kailash Nadh -- boastMachine	Cross-site scripting (XSS) vulnerability in (1) index.php and (2) bmc/admin.php in BoastMachine (bMachine) 3.1 and earlier allows remote attackers to inject arbitrary web script or HTML via the query string, which is not properly filtered when it is accessed using the $_SERVER["PHP_SELF"] variable.	unknown 2006-05-19	7.0	CVE-2006-2491 BUGTRAQ BID FRSIRT SECUNIA OSVDB OSVDB XF
CaLogic -- CaLogic Calendars	PHP remote file inclusion vulnerability in CaLogic Calendars 1.2.2 allows remote attackers to execute arbitrary PHP code via a URL in the GLOBALS["CLPath"] parameter to (1) reconfig.php and (2) srxclr.php. NOTE: this might be due to a globals overwrite issue.	unknown 2006-05-24	7.0	CVE-2006-2570 OTHER-REF BID
Coppermine -- Photo Gallery	Coppermine galleries before 1.4.6, when running on Apache with mod_mime installed, allows remote attackers to upload arbitrary files via a filename with multiple file extensions.	unknown 2006-05-22	7.0	CVE-2006-2514 SOURCEFORGE FRSIRT SECUNIA
Dayfox -- Dayfox Blog	Dayfox Blog 2.0 and earlier stores user credentials in edit/slog_users.txt under the web document root with insufficient access control, which allows remote attackers to gain privileges.	unknown 2006-05-22	7.0	CVE-2006-2522 OTHER-REF FRSIRT SECUNIA
DSChat -- DSChat	Unspecified vulnerability in DSChat 1.0 allows remote attackers to execute arbitrary PHP code via the Nickname field, which is not sanitized before creating a file in a user directory. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-05-25	7.0	CVE-2006-2592 FRSIRT SECUNIA
Edimax -- BR-6104K	Edimax BR-6104K router allows remote attackers to bypass access restrictions and conduct unauthorized operations via a UPnP request with a modified InternalClient parameter (possibly within NewInternalClient), which is not validated, as demonstrated by using AddPortMapping to forward arbitrary traffic.	2006-01-30 2006-05-23	10.0	CVE-2006-2561 OTHER-REF OTHER-REF FRSIRT SECUNIA
Edimax -- BR-6104K	ZyXEL P-335WT router allows remote attackers to bypass access restrictions and conduct unauthorized operations via a UPnP request with a modified InternalClient parameter , which is not validated, as demonstrated by using AddPortMapping to forward arbitrary traffic.	2006-01-30 2006-05-23	7.0	CVE-2006-2562 OTHER-REF OTHER-REF FRSIRT SECUNIA
FreeType -- FreeType	Multiple integer overflows in FreeType before 2.2 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via attack vectors related to (1) bdf/bdflib.c, (2) sfnt/ttcmap.c, and (3) cff/cffgload.c.	unknown 2006-05-23	7.0	CVE-2006-1861 OTHER-REF OTHER-REF

Fujitsu -- MyWeb Portal Office Public Edition Fujitsu -- MyWeb Portal Office Medical Edition Fujitsu -- MyWeb Portal Office Standard Edition Fujitsu -- MyWeb Portal Office Light Edition Fujitsu -- MyWeb Portal Office School Edition Fujitsu -- MyWeb Portal Office Citizen Edition	SQL injection vulnerability in MyWeb Portal Office, Standard Edition, Public Edition, Medical Edition, Citizen Edition, School Edition, and Light Edition allows remote attackers to execute arbitrary SQL commands via unknown attack vectors.	unknown 2006-05-22	7.0	CVE-2006-2517 FRSIRT SECUNIA
Hiox -- Guestbook	Cross-site scripting (XSS) vulnerability in index.php in Hiox Guestbook 3.1 allows remote attackers to inject arbitrary web script or HTML via the input forms for signing the guestbook.	2006-05-20 2006-05-22	7.0	CVE-2006-2515 BUGTRAQ SECUNIA FRSIRT
HP -- HP-UX	Multiple unspecified vulnerabilities in Software Distributor in HP-UX B.11.00, B.11.04, B.11.11, and B.11.23 allow local users to gain privileges via unspecified attack vectors.	2006-05-23 2006-05-24	7.0	CVE-2006-2574 HP OTHER-REF FRSIRT SECTRACK SECUNIA
HP -- OpenView Storage Data Protector	Unspecified vulnerability in HP OpenView Storage Data Protector 5.1 and 5.5 allows remote attackers to execute arbitrary code via unknown vectors.	unknown 2006-05-24	7.0	CVE-2006-2579 HP OTHER-REF FRSIRT SECTRACK
HP -- OpenView Network Node Manager	Multiple unspecified vulnerabilities in HP OpenView Network Node Manager (OV NNM) 6.20, 6.4x, 7.01, and 7.50 allow remote attackers to gain privileged access, execute arbitrary commands, or create arbitrary files via unknown vectors.	unknown 2006-05-24	7.0	CVE-2006-2580 HP OTHER-REF FRSIRT SECTRACK SECUNIA
HyperStop -- WebHost Directory AlstraSoft -- WebHost Directory	SQL injection vulnerability in the search script in (1) AlstraSoft Web Host Directory 1.2, aka (2) HyperStop WebHost Directory 1.2, allows remote attackers to execute arbitrary SQL commands via the uri parameter.	unknown 2006-05-25	7.0	CVE-2006-2616 BUGTRAQ FRSIRT FRSIRT SECUNIA SECUNIA
Ipswitch -- WhatsUp	Ipswitch WhatsUp Professional 2006 only verifies the users identity via HTTP headers, which allows remote attackers to spoof being a trusted console and bypass authentication by setting HTTP User-Agent header to "Ipswitch/1.0" and the User-Application header to "NmConsole".	2006-05-17 2006-05-22	7.0	CVE-2006-2531 BUGTRAQ BUGTRAQ OTHER-REF
Linksys -- WRT54G	Linksys WRT54G Wireless-G Broadband Router allows remote attackers to bypass access restrictions and conduct unauthorized operations via a UPnP request with a modified InternalClient parameter, which is not validated, as demonstrated by using AddPortMapping to forward arbitrary traffic.	2006-01-30 2006-05-23	7.0	CVE-2006-2559 OTHER-REF OTHER-REF FRSIRT SECUNIA
Paul Vixie -- Vixie Cron	do_command.c in Vixie cron (vixie-cron) 4.1 does not check the return code of a setuid call, which might allow local users to gain root privileges if setuid fails in cases such as PAM failures or resource limits.	unknown 2006-05-25	7.0	CVE-2006-2607 OTHER-REF OTHER-REF
PDF Tools AG -- PDF Form Filling and Flattening Tool	Stack-based buffer overflow in PDF Form Filling and Flattening Tool before 3.1.0.12 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via long field names.	2006-04-19 2006-05-24	7.0	CVE-2006-2549 OTHER-REF FRSIRT SECUNIA
perlpodder -- perlpodder Prodder -- Prodder	Prodder before 0.5, and perlpodder before 0.5, allows remote attackers to execute arbitrary code via shell metacharacters in the URL of a podcast, which are executed when running wget.	2006-05-18 2006-05-23	7.0	CVE-2006-2548 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECUNIA SECUNIA
phpMyDirectory -- phpMyDirectory	PHP remote file inclusion vulnerability in cron.php in phpMyDirectory 10.4.4 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the ROOT_PATH parameter.	unknown 2006-05-22	7.0	CVE-2006-2521 OTHER-REF FRSIRT SECUNIA

PostgreSQL -- PostgreSQL	PostgreSQL 8.1.x before 8.1.4, 8.0.x before 8.0.8, 7.4.x before 7.4.13, 7.3.x before 7.3.15, and earlier versions allows context-dependent attackers to bypass SQL injection protection methods in applications via invalid encodings of multibyte characters, aka one variant of "Encoding-Based SQL Injection."	unknown 2006-05-24	7.0	CVE-2006-2313 MLIST OTHER-REF FRSIRT REDHAT
PostgreSQL -- PostgreSQL	PostgreSQL 8.1.x before 8.1.4, 8.0.x before 8.0.8, 7.4.x before 7.4.13, 7.3.x before 7.3.15, and earlier versions allows context-dependent attackers to bypass SQL injection protection methods in applications that use multibyte encodings that allow the "\" (backslash) byte 0x5c to be the trailing byte of a multibyte character, such as SJIS, BIG5, GBK, GB18030, and UHC, which cannot be handled correctly by a client that does not understand multibyte encodings, aka a second variant of "Encoding-Based SQL Injection." NOTE: it could be argued that this is a class of issue related to interaction errors between the client and PostgreSQL, but a CVE has been assigned since PostgreSQL is treating this as a preventative measure against this class of problem.	unknown 2006-05-24	7.0	CVE-2006-2314 MLIST OTHER-REF FRSIRT REDHAT
Russcom Network -- Russcom.Ping	ping.php in Russcom.Ping allows remote attackers to execute arbitrary commands via shell metacharacters in the domain parameter.	2006-05-21 2006-05-25	7.0	CVE-2006-2615 BUGTRAQ BID FRSIRT SECUNIA
RWiki -- RWiki	The editing form in RWiki 2.1.0pre1 through 2.1.0 allows remote attackers to execute arbitrary Ruby code via unknown attack vectors.	unknown 2006-05-25	7.0	CVE-2006-2582 FRSIRT SECUNIA
SAP -- sapdba	Unspecified vulnerability in the sapdba command in SAP with Informix before 700, and 700 up to patch 100, allows local users to execute arbitrary commands via unknown vectors related to "insecure environment variable" handling.	2006-04-20 2006-05-23	7.0	CVE-2006-2547 FULLDISC OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
Senile Team -- Beats of Rage Horizontal Shooter BOR -- Horizontal Shooter BOR OpenBOR -- OpenBOR	Multiple format string vulnerabilities in (a) OpenBOR 2.0046 and earlier, (b) Beats of Rage (BOR) 1.0029 and earlier, and (c) Horizontal Shooter BOR (HOR) 2.0000 and earlier allow remote attackers to execute code via format string specifiers in configurations used in various mod files, as demonstrated by the (1) music identifier in data/scenes/intro.txt, which is not properly handled in the update function, and (2) background identifier in data/easy/1aeasy.txt, which is not properly handled in the shutdown function.	unknown 2006-05-22	7.0	CVE-2006-2537 OTHER-REF FRSIRT FRSIRT FRSIRT SECUNIA SECUNIA SECUNIA BID
Sitecom -- WL-153	Sitecom WL-153 router firmware before 1.38 allows remote attackers to bypass access restrictions and conduct unauthorized operations via a UPnP request with a modified InternalClient parameter, which is not validated, as demonstrated by using AddPortMapping to forward arbitrary traffic.	2006-01-30 2006-05-23	7.0	CVE-2006-2560 OTHER-REF OTHER-REF FRSIRT SECUNIA
SmartISoft -- phpListPro	PHP remote file inclusion vulnerability in config.php in phpListPro 2.0.1 and earlier, with magic_quotes_gpc disabled, allows remote attackers to execute arbitrary PHP code via a URL in the Language cookie.	unknown 2006-05-22	7.0	CVE-2006-2523 OTHER-REF FRSIRT SECUNIA
SmartISoft -- phpBazar	Admin/admin.php in phpBazar 2.1.0 and earlier allows remote attackers to bypass the authentication process and gain unauthorized access to the administrative section by setting the action parameter to edit_member and the value parameter to 1.	2006-05-20 2006-05-22	7.0	CVE-2006-2527 BUGTRAQ BID FRSIRT
Sun -- Java System Directory Server	Unspecified vulnerability in the installation process in Sun Java System Directory Server 5.2 causes wrong user data to be written to a file created by the installation, which allows remote attackers or local users to gain privileges.	unknown 2006-05-22	7.0	CVE-2006-2513 SUNALERT BID FRSIRT SECTRACK SECUNIA XF
UseBB -- UseBB	Cross-site scripting (XSS) vulnerability in UseBB 1.0 RC1 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors when processing the user date format.	2006-05-20 2006-05-22	7.0	CVE-2006-2524 OTHER-REF OTHER-REF FRSIRT SECUNIA
Woltlab -- Burning Board 4R Linklist -- 4R Linklist	SQL injection vulnerability in links.php in 4R Linklist 1.0 RC2 and earlier, a module for Woltlab Burning Board, allows remote attackers to execute arbitrary SQL commands via the cat parameter.	2006-05-20 2006-05-24	7.0	CVE-2006-2569 OTHER-REF BID FRSIRT

				SECUNIA
YourFreeWorld -- Short Url & Url Tracker Script	SQL injection vulnerability in login.php in YourFreeWorld.com Short Url & Url Tracker Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-05-22	7.0	CVE-2006-2509 BUGTRAQ BID
Zixforum -- Zixforum	SQL injection vulnerability in settings.asp in Zixforum 1.12 allows remote attackers to execute arbitrary SQL commands via the layid parameter to (1) login.asp and (2) main.asp.	unknown 2006-05-23	7.0	CVE-2006-2541 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Artmedic Webdesign -- Artmedic Newsletter	artmedic newsletter 4.1 and possibly other versions, when register_globals is enabled, allows remote attackers to modify arbitrary files and execute arbitrary PHP code via the logfile parameter in a direct request to log.php, which causes the $logfile variable to be redefined to an attacker-controlled value, as demonstrated by injecting PHP code into info.php.	unknown 2006-05-25	5.6	CVE-2006-2608 BUGTRAQ BID FRSIRT SECUNIA
Artmedic Webdesign -- Artmedic Newsletter	artmedic newsletter 4.1.2 and possibly other versions, when register_globals is enabled, allows remote attackers to modify arbitrary files and execute arbitrary PHP code via the email parameter to newsletter_log.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-05-25	5.6	CVE-2006-2609 FRSIRT SECUNIA
ASPBB -- ASPBB	Multiple cross-site scripting (XSS) vulnerabilities in AspBB 0.5.2 allow remote attackers to inject arbitrary web script or HTML via the (1) action parameter to default.asp or (2) get parameter to profile.asp.	2006-05-18 2006-05-19	4.7	CVE-2006-2497 BUGTRAQ BID SECUNIA XF
Destiney -- Destiney Rated Images Script	stats.php in Destiney Rated Images Script 0.5.0 allows remote attackers to obtain the installation path via an invalid s parameter, which displays the path in an error message. NOTE: this issue was originally claimed to be SQL injection, but CVE analysis shows that the problem is related to an invalid value that prevents some variables from being set.	2006-05-21 2006-05-22	4.7	CVE-2006-2532 BUGTRAQ
Destiney -- Destiney Rated Images Script	Cross-site scripting (XSS) vulnerability in (1) addWeblog.php and (2) leaveComments.php in Destiney Rated Images Script 0.5.0 does not properly filter all vulnerable HTML tags, which allows remote attackers to inject arbitrary web script or HTML via Javascript in a DIV tag.	2006-05-18 2006-05-22	4.7	CVE-2006-2533 BUGTRAQ BID FRSIRT SECUNIA
Destiney -- Destiney Links Script	Cross-site scripting (XSS) vulnerability in Destiney Links Script 2.1.2 allows remote attackers to inject arbitrary web script or HTML via the (1) "Search" (term parameter in index.php) and (2) "Add a Site" (add.php) fields.	2006-05-18 2006-05-22	4.7	CVE-2006-2536 BUGTRAQ BID FRSIRT SECUNIA
Destiney -- Destiney Links Script	SQL injection vulnerability in Destiney Links Script 2.1.2 allows remote attackers to execute arbitrary SQL commands via the ID parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2006-05-23 2006-05-25	4.7	CVE-2006-2585 FRSIRT SECUNIA
DGBook -- DGBook	SQL injection vulnerability in index.php in DGBook 1.0, with magic_quotes_gpc disabled, allows remote attackers to execute arbitrary SQL commands via the (1) name, (2) email, (3) homepage, (4) address, (5) comment, and (6) ip parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-05-24	5.6	CVE-2006-2573 FRSIRT SECUNIA
Dia -- Dia	Format string vulnerability in Dia 0.94 allows user-complicit attackers to cause a denial of service (crash) and possibly execute arbitrary code by triggering errors or warnings, as demonstrated via format string specifiers in a .bmp filename. NOTE: the original exploit was demonstrated through a command line argument, but there are other mechanisms inputs that are automatically process by Dia, such as a crafted .dia file.	unknown 2006-05-19	5.6	CVE-2006-2480 VULN-DEV OTHER-REF OTHER-REF SECUNIA BID FRSIRT OSVDB SECUNIA

Docebo -- Docebo	Multiple PHP remote file inclusion vulnerabilities in Docebo 3.0.3 and earlier, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in (1) GLOBALS[where_framework] to (a) lib.simplesel.php, (b) lib.filelist.php, (c) tree.documents.php, (d) lib.repo.php, and (e) lib.php, and (2) GLOBALS[where_scs] to (f) lib.teleskill.php. NOTE: this issue might be resultant from a global overwrite vulnerability.	unknown 2006-05-24	5.6	CVE-2006-2576 OTHER-REF FRSIRT SECUNIA
Docebo -- Docebo	Multiple PHP remote file inclusion vulnerabilities in Docebo 3.0.3 and earlier, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in (1) where_cms, (2) where_lms, (3) where_upgrade, (4) BBC_LIB_PATH, and (5) BBC_LANGUAGE_PATH parameters in various unspecifed scripts. NOTE: the provenance of some of this information is unknown; the details are obtained solely from third party information.	2006-05-23 2006-05-24	5.6	CVE-2006-2577 SECUNIA
e107.org -- e107 website system	SQL injection vulnerability in e107 before 0.7.5 allows remote attackers to execute arbitrary SQL commands via unknown attack vectors.	2006-05-23 2006-05-25	4.7	CVE-2006-2590 OTHER-REF FRSIRT SECUNIA
e107.org -- e107 website system	Unspecified vulnerability in e107 before 0.7.5 has unknown impact and remote attack vectors related to an "emailing exploit".	2006-05-23 2006-05-25	5.6	CVE-2006-2591 OTHER-REF FRSIRT SECUNIA
eSyndicat -- eSyndicat Directory	admin/cron.php in eSyndicat Directory 1.2, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to include arbitrary files and possibly execute arbitrary PHP code via a null-terminated value in the path_to_config parameter.	unknown 2006-05-24	5.6	CVE-2006-2578 OTHER-REF
Florian Amrhein -- NewsPortal	Cross-site scripting (XSS) vulnerability in Florian Amrhein NewsPortal before 0.37, and possibly TR Newsportal (TRanx rebuilded), allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2006-05-16 2006-05-23	4.7	CVE-2006-2556 BUGTRAQ OTHER-REF OSVDB SECUNIA FRSIRT
Florian Amrhein -- NewsPortal	PHP remote file inclusion vulnerability in extras/poll/poll.php in Florian Amrhein NewsPortal before 0.37, and TR Newsportal (TRanx rebuilded), allows remote attackers to execute arbitrary PHP code via a URL in the file_newsportal parameter.	2006-05-16 2006-05-23	4.7	CVE-2006-2557 BUGTRAQ BUGTRAQ OTHER-REF OTHER-REF BID OSVDB OSVDB SECUNIA SECUNIA XF XF FRSIRT
FrontRange -- iHEAT	The ActiveX version of FrontRange iHEAT allows remote authenticated users to run arbitrary programs or access arbitrary files on the host machine by uploading a file with an extension that is not associated with an application, and selecting a file from the "Open With..." dialog.	unknown 2006-05-22	4.2	CVE-2006-2511 BUGTRAQ SECTRACK
Genecys -- Genecys	Buffer overflow in the tell_player_surr_changes function in Genecys 0.2 and earlier might allow remote attackers to execute arbitrary code via long arguments.	2006-05-12 2006-05-23	4.7	CVE-2006-2554 FULLDISC OTHER-REF BID FRSIRT OSVDB SECUNIA XF
Hitachi -- EUR Print Service Hitachi -- EUR Professional Hitachi -- EUR Print Service for ILF Hitachi -- EUR Viewer	SQL injection vulnerability in Hitachi EUR Professional Edition, EUR Viewer, EUR Print Service, and EUR Print Service for ILF allows remote authenticated users to execute arbitrary SQL commands via unknown attack vectors.	unknown 2006-05-22	4.2	CVE-2006-2512 HITACHI BID FRSIRT SECUNIA XF OSVDB
IpLogger -- IpLogger	Cross-site scripting (XSS) vulnerability in IpLogger 1.7 and earlier allows remote attackers to inject arbitrary HTML or web script via the User-Agent (useragent) header in an HTTP request, which is not filtered when the log files are viewed.	2006-05-22 2006-05-23	4.7	CVE-2006-2558 BUGTRAQ BID FRSIRT SECUNIA

IpLogger -- IpLogger	Cross-site scripting (XSS) vulnerability in IpLogger 1.7 and earlier allows remote attackers to inject arbitrary HTML or web script via the HTTP_REFERER header in an HTTP request.	2006-05-23 2006-05-25	4.7	CVE-2006-2586 FRSIRT
libspf -- libspf	Format string vulnerability in ANSI C Sender Policy Framework library (libspf) before 1.0.0-p5, when debugging is enabled, allows remote attackers to execute arbitrary code via format string specifiers, possibly in an e-mail address.	2006-05-09 2006-05-22	4.7	CVE-2006-1520 OTHER-REF OTHER-REF OTHER-REF FRSIRT XF
MyBulletinBoard -- MyBulletinBoard	SQL injection vulnerability in rss.php in MyBB (aka MyBulletinBoard) 1.1.1 allows remote attackers to execute arbitrary SQL commands via the comma parameter. NOTE: it is not clear from the original report how this attack can succeed, since the demonstration URL uses a variable that is overwritten with static data in the extracted source code.	2006-05-18 2006-05-25	4.7	CVE-2006-2589 BUGTRAQ
Nucleus Group -- Nucleus CMS	PHP remote file inclusion vulnerability in nucleus/libs/PLUGINADMIN.php in Nucleus 3.22 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[DIR_LIBS] parameter.	unknown 2006-05-25	5.6	CVE-2006-2583 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF FRSIRT SECUNIA
perlpodder -- perlpodder	perlpodder before 0.5 allows remote attackers to execute arbitrary code via shell metacharacters in the URL of a podcast, which are executed when saving the URL to a log file. NOTE: the wget vector is already covered by CVE-2006-2548.	unknown 2006-05-23	5.6	CVE-2006-2550 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Power Place -- PHP Easy Galerie	PHP remote file inclusion vulnerability in index.php in PHP Easy Galerie 1.1 allows remote attackers to execute arbitrary PHP code via a URL in the includepath parameter.	2006-05-21 2006-05-22	4.7	CVE-2006-2526 BUGTRAQ BID SECUNIA
SmartISoft -- phpBazar	PHP remote file inclusion vulnerability in classified_right.php in phpBazar 2.1.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the language_dir parameter.	2006-05-20 2006-05-22	4.7	CVE-2006-2528 BUGTRAQ BID SECUNIA
Sun -- N1 System Manager	Sun N1 System Manager 1.1 for Solaris 10 before patch 121161-01 records system passwords in the world-readable scripts (1) /cr/hd_jobs_db.sh, (2) /cr/hd_plan_checkin.sh, and (3) /cr/oracle_plan_checkin.sh, which allows local users to obtain System Manager passwords.	unknown 2006-05-25	4.9	CVE-2006-2614 SUNALERT FRSIRT SECTRACK SECUNIA XF
Sybase -- EAServer	Sybase EAServer 5.0 for HP-UX Itanium, 5.2 for IBM AIX, HP-UX PA-RISC, Linux x86, and Sun Solaris SPARC, and 5.3 for Sun Solaris SPARC does not properly protect passwords when they are being entered via the GUI, which allows local users to obtain the cleartext passwords via the getSelectedText function in javax.swing.JPasswordField component.	2006-04-13 2006-05-22	5.6	CVE-2006-2539 OTHER-REF BID FRSIRT SECUNIA
UBBCentral -- UBB.Threads	PHP remote file inclusion vulnerability in addpost_newpoll.php in UBB.threads 6.4 through 6.5.2 and 6.5.1.1 (trial) allows remote attackers to execute arbitrary PHP code via a URL in the thispath parameter.	2006-04-20 2006-05-24	5.6	CVE-2006-2568 OTHER-REF FRSIRT SECUNIA
UseBB -- UseBB	SQL injection vulnerability in UseBB 1.0 RC1 and earlier allows remote attackers to execute arbitrary SQL commands via the member list search module.	2006-05-20 2006-05-22	4.7	CVE-2006-2525 OTHER-REF OTHER-REF FRSIRT SECUNIA
XOOPS -- XOOPS	mainfile.php in XOOPS 2.0.13.2 and earlier, when register_globals is enabled, allows remote attackers to overwrite variables such as $xoopsOption['nocommon'] and conduct directory traversal attacks or include PHP files via (1) xoopsConfig[language] to misc.php or 92) xoopsConfig[theme_set] to index.php, as demonstrated by injecting PHP sequences into a log file.	2006-05-21 2006-05-22	5.6	CVE-2006-2516 BUGTRAQ Milw0rm FRSIRT SECUNIA BID OSVDB
Xtreme Scripts -- Xtreme Topsites	Xtreme Topsites 1.1 allows remote attackers to trigger MySQL errors and possibly conduct SQL injection attacks via unspecified vectors in join.php.	unknown 2006-05-23	5.6	CVE-2006-2543 BUGTRAQ BID FRSIRT SECUNIA

Xtreme Scripts -- Xtreme Topsites	Multiple SQL injection vulnerabilities in Xtreme Topsites 1.1, with magic_quotes_gpc disabled, allow remote attackers to execute arbitrary SQL commands via the (1) searchthis parameter in lostid.php and (2) id parameter in stats.php. NOTE: the provenance of this information is unknown; portions of the details are obtained from third party information.	unknown 2006-05-23	5.6	CVE-2006-2544 FRSIRT SECUNIA

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Alkacon -- OpenCms	Cross-site scripting (XSS) vulnerability in search.html in Alkacon OpenCms 6.0.0, 6.0.2, and 6.0.3 allows remote attackers to inject arbitrary web script or HTML via the query parameter in a search action.	unknown 2006-05-24	1.9	CVE-2006-2571 OTHER-REF SECUNIA
AlstraSoft -- E-Friends	Multiple cross-site scripting (XSS) vulnerabilities in index.php in AlstraSoft E-Friends allow remote attackers to inject arbitrary web script or HTML by (1) posting a blog, (2) posting a listing, (3) posting an event, (4) adding comments, or (5) sending a message.	unknown 2006-05-24	2.3	CVE-2006-2564 BUGTRAQ BID FRSIRT SECUNIA
AlstraSoft -- Article Manager Pro	Alstrasoft Article Manager Pro 1.6 allows remote attackers to obtain sensitive information via (1) a quote character or possibly an invalid value in the action parameter in a request to mrarticles.php or (2) a login QUERY_STRING to admin.php without any additional parameters, which reveal the path in various error messages.	unknown 2006-05-24	2.3	CVE-2006-2566 BUGTRAQ FRSIRT
AlstraSoft -- Article Manager Pro	Cross-site scripting (XSS) vulnerability in submit_article.php in Alstrasoft Article Manager Pro 1.6 allows remote attackers to inject arbitrary web script or HTML when submitting an article, as demonstrated using a javascript URI in a Cascading Style Sheets (CSS) property of a STYLE attribute of an element.	unknown 2006-05-24	2.3	CVE-2006-2567 BUGTRAQ FRSIRT SECUNIA
Apple -- Mac OS X Apple -- Xcode Tools	Xcode Tools before 2.3 for Mac OS X 10.4, when running the WebObjects plugin, allows remote attackers to access or modify WebObjects projects through a network service.	unknown 2006-05-23	3.7	CVE-2006-1466 APPLE BID FRSIRT SECTRACK
BEA Systems -- WebLogic Server	A recommended admin password reset mechanism for BEA WebLogic Server 8.1, when followed before October 10, 2005, causes the administrator password to be stored in cleartext in the domain directory, which could allow attackers to gain privileges.	unknown 2006-05-23	2.3	CVE-2006-2546 BEA FRSIRT SECTRACK SECUNIA XF
Bitberry Software -- BitZipper	Directory traversal vulnerability in BitZipper 4.1.2 SR-1 and earlier allows remote attackers to create files in arbitrary directories via a .. (dot dot) in the filename of a file that is stored in a (1) RAR (.rar), (2) TAR (.tar), (3) ZIP (.zip), (4) GZ (.gz), or (5) JAR (.jar) archive.	unknown 2006-05-22	2.3	CVE-2006-2520 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA SECTRACK
Chatty -- Chatty	Cross-site scripting (XSS) vulnerability in Chatty, possibly 1.0.2 and other versions, allows remote attackers to inject arbitrary web script or HTML via the username.	2006-05-21 2006-05-25	2.3	CVE-2006-2606 BUGTRAQ BID
Destiney -- Destiney Links Script	Destiney Links Script 2.1.2 does not protect library and other support files, which allows remote attackers to obtain the installation path via a direct URL to files in the (1) include and (2) themes/original directories.	2006-05-18 2006-05-22	2.3	CVE-2006-2534 BUGTRAQ
Destiney -- Destiney Links Script	index.php in Destiney Links Script 2.1.2 allows remote attackers to obtain the installation path via an invalid show parameter referencing a non-existent file, which reveals the path in the resulting error message. NOTE: this issue might be resultant from a more serious issue such as directory traversal.	2006-05-18 2006-05-22	2.3	CVE-2006-2535 BUGTRAQ FRSIRT SECUNIA
Dian Gemilang -- DGBook	Cross-site scripting (XSS) vulnerability in index.php in DGBook 1.0 allows remote attackers to inject arbitrary web script or HTML via the (1) name, (2) homepage, (3) email, and (4) address parameters.	unknown 2006-05-24	1.9	CVE-2006-2572 BUGTRAQ FRSIRT SECUNIA
DieselScripts.com -- Diesel Job Site	Privacy leak in install.php for Diesel PHP Job Site sends sensitive information such as user credentials to an e-mail address controlled by the product developers.	unknown 2006-05-23	2.3	CVE-2006-2540 BUGTRAQ SECUNIA
DSChat -- DSChat	Cross-site scripting (XSS) vulnerability in DSChat 1.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the chatbox, probably involving the ctext parameter to send.php.	2006-05-21 2006-05-25	2.3	CVE-2006-2605 BUGTRAQ BID FRSIRT

				SECUNIA
FCKeditor -- FCKeditor	editor/filemanager/upload/php/upload.php in FCKeditor before 2.3 Beta, when the upload feature is enabled, does not verify the Type parameter, which allows remote attackers to upload arbitrary file types. NOTE: It is not clear whether this is related to CVE-2006-0658.	2006-05-18 2006-05-22	2.3	CVE-2006-2529 OTHER-REF BID FRSIRT SECUNIA
FreeType -- FreeType	integer underflow in Freetype before 2.2 allows remote attackers to cause a denial of service (crash) via a font file with an odd number of blue values, which causes the underflow when decrementing by 2 in a context that assumes an even number of values.	2006-03-02 2006-05-23	2.3	CVE-2006-0747 OTHER-REF
FreeType -- FreeType	Integer overflow in the read_lwfn function in FreeType before 2.2 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted LWFN file. NOTE: this issue might be subsumed by CVE-2006-1861.	unknown 2006-05-19	3.3	CVE-2006-2493 SOURCEFORGE FRSIRT SECUNIA BID XF
Genecys -- Genecys	The parse_command function in Genecys 0.2 and earlier allows remote attackers to cause a denial of service (crash) via a command with a missing ":" (colon) separator, which triggers a null dereference.	2006-05-12 2006-05-23	2.3	CVE-2006-2555 FULLDISC OTHER-REF BID FRSIRT OSVDB SECUNIA XF
HP -- HP-UX	Unspecified vulnerability in the kernel in HP-UX B.11.00 allows local users to cause an unspecified denial of service via unknown vectors.	unknown 2006-05-23	1.6	CVE-2006-2551 HP BID FRSIRT SECUNIA
HyperStop -- WebHost Directory AlstraSoft -- WebHost Directory	(1) AlstraSoft Web Host Directory 1.2, aka (2) HyperStop WebHost Directory 1.2, allows remote attackers to obtain the installation path via an invalid entry in the Username field on the login page, which causes the path to be displayed in an SQL error. NOTE: this issue might be resultant from SQL injection.	unknown 2006-05-25	2.3	CVE-2006-2617 BUGTRAQ OTHER-REF FRSIRT FRSIRT SECUNIA SECUNIA
HyperStop -- WebHost Directory AlstraSoft -- WebHost Directory	Cross-site scripting (XSS) vulnerability in (1) AlstraSoft Web Host Directory 1.2, aka (2) HyperStop WebHost Directory 1.2, might allow remote attackers to inject arbitrary web script or HTML via the user review box. NOTE: since user reviews do not require administrator privileges, and an auto-approve mechanism exists, this issue is a vulnerability.	unknown 2006-05-25	2.3	CVE-2006-2618 BUGTRAQ OTHER-REF
Jemscripts -- DownloadControl	Jemscripts DownloadControl 1.0 allows remote attackers to obtain sensitive information via an invalid dcid parameter to dc.php, which leaks the pathname in an error message. NOTE: this was originally claimed to be SQL injection, but it is probably resultant from another issue in functions.php.	unknown 2006-05-23	2.3	CVE-2006-2552 BUGTRAQ BID
Jemscripts -- DownloadControl	Cross-site scripting (XSS) vulnerability in Jemscripts DownloadControl 1.0 allows remote attackers to inject arbitrary HTML or web script via the dcid parameter to dc.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. This issue appears to be independent from a different issue that involves the same vector.	2006-05-23 2006-05-23	2.3	CVE-2006-2553 BUGTRAQ MLIST SECUNIA
Linux -- Linux kernel	The virtual memory implementation in Linux kernel 2.6.x allows local users to cause a denial of service (panic) by running lsof a large number of times in a way that produces a heavy system load.	unknown 2006-05-24	2.3	CVE-2006-1862 REDHAT OTHER-REF OTHER-REF SECUNIA
Linux -- Linux kernel	The snmp_trap_decode function in the SNMP NAT helper for Linux kernel before 2.6.16.18 allows remote attackers to cause a denial of service (crash) via unspecified remote attack vectors that cause failures in snmp_trap_decode that trigger (1) frees of random memory or (2) frees of previously-freed memory (double-free) by snmp_trap_decode as well as its calling function, as demonstrated via certain test cases of the PROTOS SNMP test suite.	unknown 2006-05-25	3.3	CVE-2006-2444 KERNEL.ORG KERNEL.ORG SECUNIA
MediaWiki -- MediaWiki	Cross-site scripting (XSS) vulnerability in includes/Sanitizer.php in the variable handler in MediaWiki 1.6.x before r14349 allows remote attackers to inject arbitrary Javascript via unspecified vectors, possibly involving the usage of the | (pipe) character.	unknown 2006-05-25	2.3	CVE-2006-2611 MLIST MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF FRSIRT

				SECUNIA
Mozilla -- Firefox IE Tab -- IE Tab	IE Tab 1.0.9 plugin for Mozilla Firefox 1.5.0.3 allows remote user-complicit attackers to cause a denial of service (application crash), possibly due to a null dereference, via certain Javascript, as demonstrated using a url parameter to the content/reloaded.html page in a chrome:// URI. Some third-party researchers claim that they are unable to reproduce this vulnerability.	unknown 2006-05-22	1.9	CVE-2006-2538 BUGTRAQ BUGTRAQ XF
Mozilla -- Firefox Netscape -- Netscape Mozilla -- Mozilla Suite	Mozilla Suite 1.7.13, Mozilla Firefox before 1.8.0, and Netscape 7.2 and 8.1, and possibly other versions and products, allows remote user-complicit attackers to obtain information such as the installation path by causing exceptions to be thrown and checking the message contents.	unknown 2006-05-25	1.9	CVE-2006-2613 BUGTRAQ OTHER-REF OTHER-REF SECUNIA SECUNIA SECUNIA
Novell -- Novell client	Novell Client for Windows 4.8 and 4.9 does not restrict access to the clipboard contents while a machine is locked, which allows users with physical access to read the current clipboard contents by pasting them into the "User Name" field on the login prompt.	2006-05-21 2006-05-25	1.6	CVE-2006-2612 BUGTRAQ BUGTRAQ SECUNIA
phpwcms -- phpwcms	Cross-site scripting (XSS) vulnerability in phpwcms 1.2.5-DEV allows remote attackers to inject arbitrary web script or HTML via the BL[be_cnt_plainhtml] parameter to include/inc_tmpl/content/cnt6.inc.php.	unknown 2006-05-22	1.9	CVE-2006-2518 BUGTRAQ OTHER-REF BID SECUNIA
phpwcms -- phpwcms	Directory traversal vulnerability in include/inc_ext/spaw/spaw_control.class.php in phpwcms 1.2.5-DEV allows remote attackers to include arbitrary local files via .. (dot dot) sequences in the spaw_root parameter.	unknown 2006-05-22	1.9	CVE-2006-2519 BUGTRAQ OTHER-REF BID SECUNIA
PunkBuster -- PunkBuster	Buffer overflow in the WebTool HTTP server component in (1) PunkBuster before 1.229, as used by multiple products including (2) America's Army 1.228 and earlier, (3) Battlefield 1942 1.158 and earlier, (4) Battlefield 2 1.184 and earlier, (5) Battlefield Vietnam 1.150 and earlier, (6) Call of Duty 1.173 and earlier, (7) Call of Duty 2 1.108 and earlier, (8) DOOM 3 1.159 and earlier, (9) Enemy Territory 1.167 and earlier, (10) Far Cry 1.150 and earlier, (11) F.E.A.R. 1.093 and earlier, (12) Joint Operations 1.187 and earlier, (13) Quake III Arena 1.150 and earlier, (14) Quake 4 1.181 and earlier, (15) Rainbow Six 3: Raven Shield 1.169 and earlier, (16) Rainbow Six 4: Lockdown 1.093 and earlier, (17) Return to Castle Wolfenstein 1.175 and earlier, and (18) Soldier of Fortune II 1.183 and earlier allows remote attackers to cause a denial of service (application crash) via a long webkey parameter.	2006-05-23 2006-05-25	2.3	CVE-2006-2587 OTHER-REF OTHER-REF FRSIRT SECUNIA
PyroSoft Inc -- NetPanzer	The setFrame function in Lib/2D/Surface.hpp for NetPanzer 0.8 and earlier allows remote attackers to cause a denial of service (crash) via a client flag (frameNum) that is greater than 41, which triggers an assert error.	2006-05-24 2006-05-24	2.3	CVE-2006-2575 OTHER-REF FRSIRT SECUNIA
Russcom Network -- PhpImages	Russcom PHPImages allows remote attackers to upload files of arbitrary types by uploading a file with a .gif extension. NOTE: due to lack of specific information about attack vectors do not depend on the existence of another vulnerability, it is not clear whether this is a vulnerability.	2006-05-21 2006-05-25	2.3	CVE-2006-2588 BUGTRAQ BID
RWiki -- RWiki	Cross-site scripting (XSS) vulnerability in Wiki content in RWiki 2.1.0pre1 through 2.1.0 allows remote attackers to inject arbitrary web script or HTML via unknown attack vectors.	unknown 2006-05-25	2.3	CVE-2006-2581 FRSIRT SECUNIA
SkyeBox -- SkyeBox	Multiple cross-site scripting (XSS) vulnerabilities in post.php in SkyeBox 1.2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) name or (2) message parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information, although it was likely prompted by a vague announcement from a researcher who incorrectly referred to the product as "SkyeShoutbox."	unknown 2006-05-25	2.3	CVE-2006-2584 BUGTRAQ FRSIRT SECUNIA
Snitz Forums 2000 -- Avatar MOD	avatar_upload.asp in Avatar MOD 1.3 for Snitz Forums 3.4, and possibly other versions, allows remote attackers to bypass file type checks and upload arbitrary files via a null byte in the file name, as discovered by the Codescan product.	2006-05-18 2006-05-22	2.3	CVE-2006-2530 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECUNIA XF
SpiffyJr -- phpRaid	Cross-site scripting (XSS) vulnerability in view.php in phpRaid 2.9.5 allows remote attackers to inject arbitrary web script or HTML via the (1) URL query string and the (2) Sort parameter.	2006-05-19 2006-05-25	1.9	CVE-2006-2610 BUGTRAQ BID

Ti Kan -- Xmcd	xmcdconfig in Debian GNU/Linux 2.6-17.1 creates /var/lib/cddb and /var/lib/xmcd/discog with world writable permissions, which allows local users to cause a denial of service (disk consumption).	2006-05-11 2006-05-23	2.5	CVE-2006-2542 OTHER-REF SECUNIA XF
Xtreme Scripts -- Xtreme Topsites	Multiple cross-site scripting (XSS) vulnerabilities in Xtreme Topsites 1.1 allow remote attackers to inject arbitrary web script or HTML via the (1) id parameter in stats.php and (2) unspecified inputs in lostid.php, probably searchthis parameter. NOTE: one or more of these vectors might be resultant from SQL injection.	unknown 2006-05-23	1.9	CVE-2006-2545 BUGTRAQ BID FRSIRT SECUNIA
YourFreeWorld -- Short Url & Url Tracker Script	Cross-site scripting (XSS) vulnerability in the URL submission form in YourFreeWorld.com Short Url & Url Tracker Script allows remote attackers to inject arbitrary web script or HTML via unspecified form fields.	unknown 2006-05-22	2.3	CVE-2006-2510 BUGTRAQ BID

Back to top

Last updated May 29, 2006