



Search US-CERT

GO

Advanced Options...

National Cyber Alert System

Cyber Security Bulletin SB07-176

Archive

Vulnerability Summary for the Week of June 18, 2007

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
	Multiple buffer overflows in RealNetworks GameHouse	unknown	8.0	CVE-2007-2924

dldisplay ActiveX control (ghdctl.dll) allow remote attackers to execute arbitrary code via unknown vectors.	2007-06-19		CERT-VN
Unspecified vulnerability in the Default Messaging Component in IBM WebSphere Application Server (WAS) 6.1.0.7 and earlier has unknown impact and attack vectors, related to "incorrect authorization on a remote interface to the SDO repository."	unknown 2007-06-19	10.0	CVE-2007-3263 OTHER-REF FRSIRT SECUNIA
Unspecified vulnerability in the PD tools component in IBM WebSphere Application Server (WAS) 6.1.0.7 and earlier has unknown impact and attack vectors.	unknown 2007-06-19	10.0	CVE-2007-3264 OTHER-REF FRSIRT SECUNIA
Directory traversal vulnerability in webif.cgi in ifnet WEBIF allows remote attackers to include and execute arbitrary local files a .. (dot dot) in the outconfig parameter.	unknown 2007-06-19	10.0	CVE-2007-3266 BUGTRAQ OTHER-REF BID
PHP remote file inclusion vulnerability in Includes/global.inc.php in phpMyInventory 2.8 allows remote attackers to execute arbitrary PHP code via a URL in the strIncludePrefix parameter.	unknown 2007-06-19	10.0	CVE-2007-3270 MILWORM BID
PHP remote file inclusion vulnerability in templates/2blue/bodyTemplate.php in YourFreeScreamer 1.0 allows remote attackers to execute arbitrary PHP code via a URL in the serverPath parameter.	unknown 2007-06-19	7.0	CVE-2007-3271 MILWORM
SQL injection vulnerability in index.cfm in FuseTalk 2.0 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2007-06-19	7.0	CVE-2007-3273 BID
Unspecified vulnerability in the localization before 1.2 module for WIKINDX allows attackers to access certain administrative capabilities via unknown vectors.	unknown 2007-06-19	10.0	CVE-2007-3277 OTHER-REF SECUNIA

	PostgreSQL 8.1 and probably later versions, when local trust authentication is enabled and the Database Link library (dblink) is installed, allows remote attackers to access arbitrary accounts and execute arbitrary SQL queries via a dblink host parameter that proxies the connection from 127.0.0.1.	unknown 2007-06-19	8.0	CVE-2007-3278 BUGTRAQ BUGTRAQ OTHER-REF OTHER-REF
	PostgreSQL 8.1 and probably later versions, when the PL/pgSQL (plpgsql) language has been created, grants certain plpgsql privileges to the PUBLIC domain, which allows remote attackers to create and execute functions, as demonstrated by functions that perform local brute-force password guessing attacks, which may evade intrusion detection.	unknown 2007-06-19	10.0	CVE-2007-3279 BUGTRAQ OTHER-REF OTHER-REF
Cerulean Studios -- Trillian	Heap-based buffer overflow in Cerulean Studios Trillian 3.x before 3.1.6.0 allows remote attackers to execute arbitrary code via a message sent through the MSN protocol, or possibly other protocols, with a crafted UTF-8 string, which triggers improper memory allocation for word wrapping when a window width is used as a buffer size, a different vulnerability than CVE-2007-2478.	unknown 2007-06-20	10.0	CVE-2007-3305 IDEFENSE OTHER-REF BID FRSIRT SECUNIA
Cybozu Labs -- Musoo	Multiple PHP remote file inclusion vulnerabilities in Musoo 0.21 allow remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[ini_array][EXTLIB_PATH] parameter to (1) msDb.php, (2) modules/MusooTemplateLite.php, or (3) modules/SoundImporter.php.	unknown 2007-06-20	7.0	CVE-2007-3297 MILWORM
Efstratios Geroulis -- Jasmine CMS	Multiple SQL injection vulnerabilities in Jasmine CMS 1.0 allow remote attackers to execute arbitrary SQL commands via (1) the login_username parameter to login.php or (2) the item parameter to news.php.	unknown 2007-06-21	7.0	CVE-2007-3313 MILWORM BID
F-Secure -- F-Secure Anti-Virus Linux Client Security	Multiple F-Secure anti-virus products for Microsoft Windows and Linux before 20070619 allow remote attackers to bypass scanning via a crafted header in a (1) LHA or (2)	unknown 2007-06-20	8.0	CVE-2007-3300 OTHER-REF BID

F-Secure -- F-Secure Anti-Virus Linux Server Security F-secure -- Solutions based on F-secure Personal Express F-Secure -- Internet Gatekeeper F-Secure -- F-Secure Internet Security F-secure -- F-Secure Anti-Virus	RAR archive.			FRSIRT SECUNIA
FuseTalk Inc. -- FuseTalk	SQL injection vulnerability in forum/include/error/autherror.cfm in FuseTalk allows remote attackers to execute arbitrary SQL commands via the errorcode parameter. NOTE: a patch may have been released privately between April and June 2007. NOTE: this issue may overlap CVE-2007-3273.	unknown 2007-06-20	7.0	CVE-2007-3301 BUGTRAQ BID
GNOME -- Evolution	Camel (camel-imap-folder.c) in the mailer component for Evolution Data Server 1.11 allows remote IMAP servers to execute arbitrary code via a negative SEQUENCE value in GData, which is used as an array index.	unknown 2007-06-19	10.0	CVE-2007-3257 OTHER-REF
LiveCMS -- LiveCMS	categoria.php in LiveCMS 3.4 and earlier allows remote attackers to obtain sensitive information via a ' (quote) character in the cid parameter, which reveals the path in a forced SQL error message.	unknown 2007-06-20	8.0	CVE-2007-3290 MILWORM
LiveCMS -- LiveCMS	Unrestricted file upload vulnerability in LiveCMS 3.4 and earlier allows remote attackers to upload and execute arbitrary PHP code by specifying a PHP file type in a parameter intended for "a small image" associated with an article.	unknown 2007-06-20	7.0	CVE-2007-3292 MILWORM
LiveCMS -- LiveCMS	SQL injection vulnerability in categoria.php in LiveCMS 3.4 and earlier allows remote attackers to execute arbitrary	unknown	7.0	CVE-2007-3293 MILWORM

	SQL commands via the cid parameter.	2007-06-20		
PHP -- PHP	Multiple buffer overflows in the Tidy extension for PHP 5.2.3 allow context-dependent attackers to execute arbitrary code via (1) a long second argument to the tidy_parse_string function or (2) an unspecified vector to the tidy_repair_string function.	unknown 2007-06-20	7.0	CVE-2007-3294 MILWORM
Simple Machines -- Simple Machines Forum	Simple Machines Forum (SMF) 1.1.2 uses a concatenation method with insufficient randomization when creating a WAV file CAPTCHA, which allows remote attackers to pass the CAPTCHA test via an automated brute-force attack.	unknown 2007-06-20	7.0	CVE-2007-3308 BUGTRAQ OTHER-REF SECTRACK XF
Simple Machines -- Simple Machines Forum	Unspecified vulnerability in Simple Machines Forum (SMF) 1.1.2 allows remote attackers to execute arbitrary PHP code during (1) creation or (2) editing of a message.	unknown 2007-06-20	7.0	CVE-2007-3309 BUGTRAQ OTHER-REF SECTRACK XF
Solar Empire -- Solar Empire	SQL injection vulnerability in game_listing.php in Solar Empire 2.9.1.1 and earlier allows remote attackers to execute arbitrary SQL commands via the User-Agent HTTP header.	unknown 2007-06-20	7.0	CVE-2007-3307 MILWORM BID
Spey -- Spey	SQL injection vulnerability in Spey before 0.4.1 allows remote attackers to execute arbitrary SQL commands via unspecified vectors related to MessageProcessor.cc and possibly other components.	unknown 2007-06-20	7.0	CVE-2007-3298 OTHER-REF OTHER-REF OTHER-REF FRSIRT
Ultrize -- MiniBill	PHP remote file inclusion vulnerability in crontab/run_billing.php in MiniBill 1.2.5 allows remote attackers to execute arbitrary PHP code via a URL in the config[include_dir] parameter, a different vector than CVE-2006-4489.	unknown 2007-06-20	7.0	CVE-2007-3306 MILWORM
VideoLAN -- VLC Media Player	Multiple format string vulnerabilities in plugins in VideoLAN VLC Media Player before 0.8.6c allow remote attackers to	unknown	8.0	CVE-2007-3316 OTHER-REF

	cause a denial of service (crash) or execute arbitrary code via format string specifiers in (1) an Ogg/Vorbis file, (2) an Ogg/Theora file, (3) a CDDB entry for a CD Digital Audio (CDDA) file, or (4) Service Announce Protocol (SAP) multicast packets.	2007-06-21		BID FRSIRT SECUNIA
Xoops -- WiwiMod Module	PHP remote file inclusion vulnerability in spaw/spaw_control.class.php in the WiwiMod 0.4 module for XOOPS allows remote attackers to execute arbitrary PHP code via a URL in the spaw_root parameter. NOTE: this issue is probably a duplicate of CVE-2006-4656.	unknown 2007-06-20	7.0	CVE-2007-3289 MILWORM
Xoops -- Articles Module	SQL injection vulnerability in print.php in the Articles 1.02 and earlier module for Xoops allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2007-06-21	7.0	CVE-2007-3311 BUGTRAQ MILWORM
Xunlei -- Web Thunderbolt	The ThunderServer.webThunder.1 ActiveX control in xunlei Web Thunderbolt 1.7.3.109 allows remote attackers to download arbitrary files and conduct other unauthorized actions by invoking dangerous methods.	unknown 2007-06-20	8.0	CVE-2007-3296 BID

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
	HP System Management Homepage (SMH) before 2.1.9 for Linux, when used with Novell eDirectory, assigns the eDirectory members to the root group, which allows remote authenticated eDirectory users to gain privileges.	unknown 2007-06-19	6.0	CVE-2007-3260 HP BID FRSIRT SECTRACK SECUNIA
	The Database Link library (dblink) in PostgreSQL 8.1 implements functions via CREATE statements that map to arbitrary libraries based on the C programming language,	unknown 2007-06-19	6.0	CVE-2007-3280 BUGTRAQ OTHER-REF

	which allows remote authenticated superusers to map and execute a function from any library, as demonstrated by using the system function in libc.so.6 to gain shell access.			OTHER-REF
Altap -- Servant Salamander Altap -- Portable Executable Viewer	Stack-based buffer overflow in peviewer.spl in Altap Servant Salamander 2.5 with Portable Executable Viewer 2.02 (English Trial), and 2.0 with Portable Executable Viewer 1.00 (English Trial), allows remote attackers to execute arbitrary code via a long PDB debug filename in a PE file.	unknown 2007-06-21	5.6	CVE-2007-3314 OTHER-REF SECUNIA
Efstratios Geroulis -- Jasmine CMS	Directory traversal vulnerability in admin/plugin_manager.php in Jasmine CMS 1.0 allows remote authenticated administrators to include and execute arbitrary local files a .. (dot dot) in the u parameter. NOTE: a separate vulnerability could be leveraged to make this issue exploitable by remote unauthenticated attackers.	unknown 2007-06-21	6.0	CVE-2007-3312 MILWORM BID
Mozilla -- Firefox	Mozilla Firefox allows remote attackers to bypass file type checks via a (1) file:/// or (2) resource: URI with a dangerous extension, followed by a nul byte (%00) and a safer extension.	unknown 2007-06-20	5.6	CVE-2007-3285 OTHER-REF BID
YaBB -- YaBB	Directory traversal vulnerability in Yet another Bulletin Board (YaBB) 2.1 and earlier allows remote authenticated users to execute arbitrary Perl code via a .. (dot dot) in the userlanguage profile setting, which sets the userlanguage key of the member hash, and is propagated to the language variable in (1) HelpCentre.pl and (2) ICQPager.pl, (3) the use_lang variable in Subs.pl, and the actlang variable in (4) Post.pl and (5) InstantMessage.pl; as demonstrated by pointing userlanguage to the English folder, modifying English/HelpCentre.lng file to contain Perl statements, and then invoking the help action in YaBB.pl.	unknown 2007-06-20	4.2	CVE-2007-3295 BUGTRAQ BID XF
YourFreeScreamer -- YourFreeScreamer	Multiple PHP remote file inclusion vulnerabilities in YourFreeScreamer 1.0, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a	unknown 2007-06-21	5.6	CVE-2007-3315 SECUNIA

URL in the serverPath parameter to bodyTemplate.php in (1) templates/Classic/, (2) templates/Classic Guestbook/, (3) templates/DarkNights/, and (4) templates/Simplistic/, different vectors than CVE-2007-3271. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
	content.php in WSPortal 1.0, when magic_quotes_gpc is disabled, allows remote attackers to obtain sensitive information via a ";" (quote semicolon) sequence in the page parameter, which reveals the installation path in the resulting forced SQL error message.	unknown 2007-06-19	2.3	CVE-2007-3127 FULLDISC OTHER-REF FRSIRT OSVDB
	SQL injection vulnerability in content.php in WSPortal 1.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the page parameter.	unknown 2007-06-19	2.3	CVE-2007-3128 FULLDISC OTHER-REF FRSIRT OSVDB
	Cross-site scripting (XSS) vulnerability in widgets/widget_search.php in dKret before 2.6 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO (PHP_SELF).	unknown 2007-06-19	2.3	CVE-2007-3261 OTHER-REF OTHER-REF FRSIRT SECUNIA
	Unspecified vulnerability in the Default Messaging Component in IBM WebSphere Application Server (WAS) 6.1.0.7 and earlier allows remote attackers to cause a denial of service related to a thread hang, and possibly related to a "TCP issue," or to MPAlarmThread and a	unknown 2007-06-19	3.3	CVE-2007-3262 OTHER-REF FRSIRT SECUNIA

	resultant memory leak.			
	Cross-site scripting (XSS) vulnerability in the Samples component in IBM WebSphere Application Server (WAS) 6.1.0.7 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2007-06-19	2.3	CVE-2007-3265 OTHER-REF FRSIRT
	Cross-site scripting (XSS) vulnerability in low.php in Fuzzylime Forum 1.01b and earlier allows remote attackers to inject arbitrary web script or HTML via the fromaction parameter in a log action, a different vector than CVE-2007-3235.	unknown 2007-06-19	2.3	CVE-2007-3267 BUGTRAQ OTHER-REF OTHER-REF
	Directory traversal vulnerability in index.php in MiniBB 2.0.5 allows remote attackers to read arbitrary files via a .. (dot dot) in the language parameter in a register action.	unknown 2007-06-19	3.3	CVE-2007-3272 MILWORM
	Apple Safari 3.0 and 3.0.1 on Windows XP SP2 allows attackers to cause a denial of service (application crash) via JavaScript that sets the document.location variable, as demonstrated by an empty value of document.location.	unknown 2007-06-19	3.3	CVE-2007-3274 BUGTRAQ
	MailWasher Server before 2.2.1, when used with LDAP or Active Directory (AD), does not properly handle blank passwords, which allows remote attackers to access an arbitrary user account and read the spam e-mail messages stored for that account. NOTE: some of these details are obtained from third party information.	unknown 2007-06-19	2.7	CVE-2007-3275 OTHER-REF SECUNIA
	Cross-site scripting (XSS) vulnerability in index.php in Site@School (S@S) 2.4.10 allows remote attackers to inject arbitrary web script or HTML via the q parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2007-06-19	2.3	CVE-2007-3276 SECUNIA
Apache Software Foundation -- Apache HTTP Server	Apache httpd 2.0.59 and 2.2.4, with the Prefork MPM module, allows local users to cause a denial of service via certain code sequences executed in a worker process that (1) stop request processing by killing all worker processes	unknown 2007-06-20	2.3	CVE-2007-3303 BUGTRAQ BUGTRAQ OTHER-REF

	and preventing creation of replacements or (2) hang the system by forcing the master process to fork an arbitrarily large number of worker processes. NOTE: This might be an inherent design limitation of Apache with respect to worker processes in hosted environments.			
Apache Software Foundation -- Apache HTTP Server	Apache httpd 1.3.37, and 2.0.59 and 2.2.4 with the Prefork MPM module, allows local users to cause a denial of service by modifying the worker_score and process_score arrays to reference an arbitrary process ID, which is sent a SIGUSR1 signal from the master process, "SIGUSR1 killer."	unknown 2007-06-20	1.9	CVE-2007-3304 BUGTRAQ BUGTRAQ OTHER-REF
Apple -- Safari	Apple Safari 3.0.1 beta (522.12.12) on Windows allows remote attackers to modify the window title and address bar while filling the main window with arbitrary content by setting the location bar and using setTimeout() to create an event that modifies the window content, which could facilitate phishing attacks.	unknown 2007-06-21	2.7	CVE-2007-2398 FULLDISC BUGTRAQ BUGTRAQ
AWFFull -- AWFFull	Cross-site scripting (XSS) vulnerability in AWFFull before 3.7.4, when AllSearchStr (aka the All Search Terms report) is enabled, allows remote attackers to inject arbitrary web script or HTML via a search string.	unknown 2007-06-20	2.3	CVE-2007-3299 MLIST MLIST MLIST OTHER-REF OTHER-REF FRSIRT
LiveCMS -- LiveCMS	Cross-site scripting (XSS) vulnerability in LiveCMS 3.4 and earlier allows remote attackers to inject arbitrary web script or HTML via an article name.	unknown 2007-06-20	1.9	CVE-2007-3291 MILWORM
Papoo -- Papoo CMS Light	Multiple cross-site scripting (XSS) vulnerabilities in Papoo Light 3.6 before 20070611 allow remote attackers to inject arbitrary web script or HTML via (1) the URI in a GET request or (2) the Title field of a visitor comment, and (3) allow remote authenticated users to inject arbitrary web script or HTML via a message to another user. NOTE:	unknown 2007-06-19	1.4	CVE-2007-3269 BUGTRAQ OTHER-REF BID

	vector (2) might overlap CVE-2006-3571.1.			
Skeltoac -- Automattic Stats	Cross-site scripting (XSS) vulnerability in the skeltoac stats (Automattic Stats) 1.0 plugin for WordPress allows remote attackers to inject arbitrary web script or HTML via the HTTP Referer field.	unknown 2007-06-20	1.9	CVE-2007-3288 BUGTRAQ BID XF
TDizin -- TDizin	Cross-site scripting (XSS) vulnerability in arama.asp in TDizin allows remote attackers to inject arbitrary web script or HTML via the ara parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2007-06-20	2.3	CVE-2007-3310 BID SECUNIA
Utopia Software -- Utopia News Pro	Cross-site scripting (XSS) vulnerability in login.php in Utopia News Pro 1.4.0 allows remote attackers to inject arbitrary web script or HTML via the password parameter.	unknown 2007-06-19	1.9	CVE-2007-3129 FULLDISC OTHER-REF OSVDB SECUNIA

[Back to top](#)

Last updated June 25, 2007