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

Also, the title of last week's bulletin incorrectly indicated that it was for the week of May 15. It actually referred to vulnerabilities recorded during the week of May 8; this bulletin references vulnerabilities recorded during the week of May 15.

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
Apple -- QuickTime	Heap-based buffer overflow in Apple QuickTime before 7.1 allows remote attackers to execute arbitrary code via a crafted BMP file that triggers the overflow in the ReadBMP function. NOTE: this issue was originally included as item 3 in CVE-2006-1983, but it has been given a separate identifier because it is a distinct issue.	unknown 2006-05-12	7.0	CVE-2006-2238 SECURITY PROTOCOLS APPLE OSVDB BID SECTRACK SECUNIA FRSIRT
BEA Systems -- Weblogic Server	The HTTP handlers in BEA WebLogic Server 9.0, 8.1 up to SP5, 7.0 up to SP6, and 6.1 up to SP7 stores the username and password in cleartext in the WebLogic Server log when access to a web application or protected JWS fails, which allows attackers to gain privileges.	2006-05-16 2006-05-19	7.0	CVE-2006-2469 BEA FRSIRT SECUNIA
BEA Systems -- Weblogic Server	Unspecified vulnerability in the WebLogic Server Administration Console for BEA WebLogic Server 9.0 prevents the console from setting custom JDBC security policies correctly, which could allow attackers to bypass intended policies.	2006-05-16 2006-05-19	7.0	CVE-2006-2470 BEA FRSIRT SECUNIA
Clam Anti-Virus -- ClamXAV Clam Anti-Virus -- ClamAV	freshclam in (1) Clam Antivirus (ClamAV) 0.88 and (2) ClamXav 1.0.3h and earlier does not drop privileges before processing the config-file command line option, which allows local users to read portions of arbitrary files when an error message displays the first line of the target file.	2006-05-15 2006-05-17	7.0	CVE-2006-2427 BUGTRAQ OTHER-REF FRSIRT SECTRACK SECUNIA
Cosmoshop -- Cosmoshop	SQL injection vulnerability in lshop.cgi in Cosmoshop 8.11.106 and earlier allows remote attackers to execute arbitrary SQL commands via the artnum parameter.	2006-05-18 2006-05-19	7.0	CVE-2006-2474 BUGTRAQ BID
e107.org -- e107 website system	SQL injection vulnerability in class2.php in e107 0.7.2 and earlier allows remote attackers to execute arbitrary SQL commands via the cookie_name cookie.	unknown 2006-05-16	7.0	CVE-2006-2416 BUGTRAQ BID FRSIRT SECUNIA OSVDB XF
EMC Corporation -- Retrospect Client	Buffer overflow in EMC Retrospect Client 5.1 through 7.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet to port 497.	2006-05-11 2006-05-15	7.0	CVE-2006-2391 OTHER-REF BID FRSIRT SECUNIA CERT-VN SECTRACK

FileZilla -- FileZilla	Buffer overflow in FileZilla before 2.2.23 allows remote attackers to execute arbitrary commands via unknown attack vectors.	unknown 2006-05-15	7.0	CVE-2006-2403 SOURCEFORGE BID FRSIRT SECUNIA
GNU -- Binutils	Buffer overflow in getsym in tekhex.c in libbfd in Free Software Foundation GNU Binutils before 20060423, as used by GNU strings, allows context-dependent attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a file with a crafted Tektronix Hex Format (TekHex) record in which the length character is not a valid hexadecimal character.	unknown 2006-05-15	7.0	CVE-2006-2362 MLIST OTHER-REF BID
IBM -- WebSphere Application Server	Unspecified vulnerability in IBM WebSphere Application Server 6.0.2, 6.0.2.1, 6.0.2.3, 6.0.2.5, and 6.0.2.7 has unknown impact and remote attack vectors related to "HTTP request handlers".	2006-05-09 2006-05-17	7.0	CVE-2006-2429 BUGTRAQ AIXAPAR OTHER-REF FRSIRT SECUNIA
IBM -- Websphere Application Server	IBM WebSphere Application Server 5.0.2 and earlier, 5.1.1 and earlier, and 6.0.2 up to 6.0.2.7 records user credentials in plaintext in addNode.log, which allows attackers to gain privileges.	2006-05-09 2006-05-17	7.0	CVE-2006-2430 BUGTRAQ AIXAPAR AIXAPAR OTHER-REF OTHER-REF OTHER-REF FRSIRT SECUNIA
IBM -- Websphere Application Server	IBM WebSphere Application Server 5.0.2 (or any earlier cumulative fix) and 5.1.1 (or any earlier cumulative fix) allows EJB access on Solaris systems via a crafted LTPA token.	2006-05-09 2006-05-17	7.0	CVE-2006-2432 BUGTRAQ OTHER-REF OTHER-REF AIXAPAR FRSIRT SECUNIA
IBM -- Websphere Application Server	WebSphere Application Server 5.0.2 (or any earlier cumulative fix) stores admin and LDAP passwords in plaintext in the FFDC logs when a login to WebSphere fails, which allows attackers to gain privileges.	2006-05-09 2006-05-17	7.0	CVE-2006-2436 BUGTRAQ OTHER-REF AIXAPAR FRSIRT SECUNIA
ImageMagick -- ImageMagick	Heap-based buffer overflow in the libMagick componet of ImageMagick 6.0.6.2 might allow attackers to execute arbitrary code via an image index array that triggers the overflow during filename glob expansion by the ExpandFilenames function.	unknown 2006-05-18	7.0	CVE-2006-2440 DEBIAN
LiveData -- ICCP Server	Heap-based buffer overflow in the ISO Transport Service over TCP (RFC 1006) implementation of LiveData ICCP Server before 5.00.035 allows remote attackers to cause a denial of service or execute arbitrary code via malformed packets.	unknown 2006-05-19	8.0	CVE-2006-0059 US-CERT CERT-VN FRSIRT OTHER-REF BID SECTRACK SECUNIA
Outgun -- Outgun	Stack-based buffer overflow in the ServerNetworking::incoming_client_data function in servnet.cpp in Outgun 1.0.3 bot 2 and earlier allows remote attackers to cause a denial of service (applicaiton crash) and possibly execute arbitrary code via a data_file_request command with a long (1) type or (2) name string.	2006-05-12 2006-05-15	7.0	CVE-2006-2399 BUGTRAQ ALTERVISTA BID FRSIRT SECUNIA
PHP Arena -- paFileDB mxBB -- mxBB Portal	PHP remote file inclusion vulnerability in pafiledb_constants.php in Download Manager (mxBB pafiledb) integration, as used with phpBB, allows remote attackers to execute arbitrary PHP code via a URL in the module_root_path parameter.	unknown 2006-05-15	7.0	CVE-2006-2361 OTHER-REF BID FRSIRT SECUNIA
phpBB Group -- phpBB	SQL injection vulnerability in charts.php in the Chart mod for phpBB allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-05-15	7.0	CVE-2006-2360 BUGTRAQ BUGTRAQ BID
Pragma Systems -- FortressSSH	Stack-based buffer overflow in Pragma FortressSSH 4.0.7.20 allows remote attackers to execute arbitrary code via long SSH_MSG_KEXINIT messages, which may cause an overflow when being logged. NOTE: the provenance of	unknown 2006-05-17	7.0	CVE-2006-2421 BID FRSIRT

	this information is unknown; the details are obtained solely from third party information.			SECUNIA
Raydium -- Raydium	Multiple buffer overflows in Raydium before SVN revision 310 allow remote attackers to execute arbitrary code via a large packet when logged via (1) the radium_log function in log.c or (2) the raydium_console_line_add function in console.c, possibly from a long player name.	unknown 2006-05-16	7.0	CVE-2006-2408 BUGTRAQ OTHER-REF OTHER-REF SECUNIA FRSIRT
Raydium -- Raydium	Buffer overflow in raydium_network_read function in network.c in Raydium SVN revision 312 and earlier allows remote attackers to execute arbitrary code by sending packets with long global variables to the client.	unknown 2006-05-16	7.0	CVE-2006-2411 BUGTRAQ OTHER-REF SECUNIA FRSIRT
RealVNC -- RealVNC	RealVNC 4.1.1, and other products that use RealVNC such as AdderLink IP, allows remote attackers to bypass authentication via a request in which the client specifies an insecure security type such as "Type 1 - None", which is accepted even if it is not offered by the server, as originally demonstrated using a long password.	2006-05-08 2006-05-15	7.0	CVE-2006-2369 OTHER-REF OTHER-REF FULLDISC MLIST OTHER-REF BUGTRAQ BUGTRAQ BUGTRAQ CERT-VN BID FRSIRT FRSIRT SECTRACK SECUNIA SECUNIA
WeOnlyDo! -- wodSSHServer freeSSHd -- freeSSHd	Stack-based buffer overflow in (1) WeOnlyDo wodSSHServer ActiveX Component 1.2.7 and 1.3.3 DEMO, as used in other products including (2) FreeSSHd 1.0.9, allows remote attackers to execute arbitrary code via a long key exchange algorithm string.	unknown 2006-05-16	7.0	CVE-2006-2407 FULLDISC BUGTRAQ BUGTRAQ BID FRSIRT FRSIRT SECUNIA SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Apple -- QuickTime Player	Stack-based buffer overflow in Apple QuickTime before 7.1 allows remote attackers to execute arbitrary code via a crafted QuickDraw PICT image format file containing malformed font information.	unknown 2006-05-12	5.6	CVE-2006-1453 BUGTRAQ APPLE APPLE CERT BID SECTRACK SECUNIA SECUNIA BID FRSIRT SECTRACK
Apple -- QuickTime Player	Heap-based buffer overflow in Apple QuickTime before 7.1 allows remote attackers to execute arbitrary code via a crafted QuickDraw PICT image format file with malformed image data.	unknown 2006-05-12	5.6	CVE-2006-1454 BUGTRAQ APPLE APPLE CERT BID SECTRACK SECUNIA SECUNIA BID FRSIRT SECTRACK

Apple -- QuickTime Player	Integer overflow in Apple QuickTime Player before 7.1 allows remote attackers to execute arbitrary code via a crafted JPEG image.	unknown 2006-05-12	5.6	CVE-2006-1458 APPLE CERT-VN BID SECTRACK SECUNIA FRSIRT
Apple -- QuickTime Player	Multiple integer overflows in Apple QuickTime before 7.1 allow remote attackers to cause a denial of service or execute arbitrary code via a crafted QuickTime movie (.MOV).	2006-05-11 2006-05-12	5.6	CVE-2006-1459 BUGTRAQ APPLE BID SECTRACK SECUNIA FRSIRT
Apple -- QuickTime Player	Multiple buffer overflows in Apple QuickTime before 7.1 allow remote attackers to execute arbitrary code via a crafted QuickTime movie (.MOV), as demonstrated via a large size for a udta Atom.	unknown 2006-05-12	5.6	CVE-2006-1460 BUGTRAQ APPLE BID SECTRACK SECUNIA BUGTRAQ OTHER-REF FRSIRT
Apple -- QuickTime Player	Multiple buffer overflows in Apple QuickTime before 7.1 allow remote attackers to execute arbitrary code via a crafted QuickTime Flash (SWF) file.	unknown 2006-05-12	5.6	CVE-2006-1461 BUGTRAQ APPLE BID SECTRACK SECUNIA FRSIRT
Apple -- QuickTime Player	Multiple integer overflows in Apple QuickTime before 7.1 allow remote attackers to execute arbitrary code via a crafted QuickTime H.264 (M4V) video format file.	unknown 2006-05-12	5.6	CVE-2006-1462 BUGTRAQ APPLE BID SECTRACK SECUNIA FRSIRT
Apple -- QuickTime Player	Heap-based buffer overflow in Apple QuickTime before 7.1 allows remote attackers to execute arbitrary code via a H.264 (M4V) video format file with a certain modified size value.	unknown 2006-05-12	5.6	CVE-2006-1463 BUGTRAQ OTHER-REF APPLE BID SECTRACK SECUNIA FRSIRT
Apple -- QuickTime Player	Buffer overflow in Apple QuickTime before 7.1 allows remote attackers to execute arbitrary code via a crafted QuickTime MPEG4 (M4P) video format file.	unknown 2006-05-12	5.6	CVE-2006-1464 BUGTRAQ APPLE BID SECTRACK SECUNIA FRSIRT
Apple -- QuickTime Player	Buffer overflow in Apple QuickTime before 7.1 allows remote attackers to execute arbitrary code via a crafted QuickTime AVI video format file.	unknown 2006-05-12	5.6	CVE-2006-1465 BUGTRAQ APPLE BID SECTRACK SECUNIA FRSIRT
BEA Systems -- Weblogic Server	stopWebLogic.sh in BEA WebLogic Server 8.1 before Service Pack 4 and 7.0 before Service Pack 6 displays the administrator password to stdout when executed, which allows local users to obtain the password by viewing a local display.	2006-05-16 2006-05-19	4.9	CVE-2006-2464 BEA FRSIRT SECTRACK SECUNIA
Blue Dragon -- PHP Blue Dragon	PHP remote file inclusion vulnerability in public_includes/pub_popup/popup_finduser.php in PHP Blue Dragon Platinum 2.8.0 allows remote attackers to execute arbitrary PHP code via a URL in the vsDragonRootPath parameter.	2006-05-15 2006-05-15	4.7	CVE-2006-2392 OTHER-REF FRSIRT SECUNIA BID

Clansys -- Clansys	Cross-site scripting (XSS) vulnerability in index.php in Clansys (aka Clanpage System) 1.1 allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2006-04-12 2006-05-15	4.7	CVE-2006-2368 BUGTRAQ OTHER-REF SECTRACK SECUNIA XF
DUware -- DUbanner	add.asp in DUware DUbanner 3.1 allows remote attackers to execute arbitrary code by uploading files with arbitrary extensions, such as ASP files, probably due to client-side enforcement that can be bypassed. NOTE: some of these details are obtained from third party information, since the raw source is vague.	2006-05-16 2006-05-17	4.7	CVE-2006-2428 BUGTRAQ BID FRSIRT SECUNIA
ezUserManager -- ezUserManager	PHP remote file inclusion vulnerability in ezUserManager 1.6 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the ezUserManager_Path parameter to ezusermanager_pwd_forgott.php, possibly due to an issue in ezusermanager_core.inc.php.	2006-05-15 2006-05-17	5.6	CVE-2006-2424 Milw0rm BID FRSIRT SECUNIA
FlexChat -- FlexChat	Multiple cross-site scripting (XSS) vulnerabilities in FlexChat 2.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) username and (2) CFTOKEN parameter in (a) index.cfm and (3) CFTOKEN and (4) CFID parameter in (b) chat.cfm.	unknown 2006-05-16	4.7	CVE-2006-2415 OTHER-REF FRSIRT SECUNIA OSVDB OSVDB SECTRACK
GPhotos -- GPhotos	Multiple cross-site scripting (XSS) vulnerabilities in GPhotos 1.5 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) rep parameter to (a) index.php or (b) diapo.php or (2) image parameter to (c) affich.php. NOTE: item 1a might be resultant from directory traversal.	2006-05-13 2006-05-15	4.7	CVE-2006-2397 BUGTRAQ BID FRSIRT SECUNIA OSVDB OSVDB OSVDB
IBM -- Websphere Application Server	Unspecified vulnerability in IBM WebSphere Application Server 5.0.2 and earlier, and 6.0.2 up to 6.0.2.7, has unknown impact and remote attack vectors related to the SOAP port.	2006-05-09 2006-05-17	4.9	CVE-2006-2431 BUGTRAQ AIXAPAR AIXAPAR OTHER-REF OTHER-REF FRSIRT SECUNIA
IBM -- WebSphere Application Server	Unspecified vulnerability in IBM WebSphere Application Server 6.0.2, 6.0.2.1, 6.0.2.3, 6.0.2.5, and 6.0.2.7 has unknown impact and attack vectors related to the "administrative console".	2006-05-09 2006-05-17	4.9	CVE-2006-2433 BUGTRAQ OTHER-REF AIXAPAR FRSIRT SECUNIA
IBM -- Websphere Application Server	Unspecified vulnerability in IBM WebSphere Application Server 5.0.2 and earlier, and 5.1.1 and earlier, has unknown impact and attack vectors related to "Inserting certain script tags in urls [that] may allow unintended execution of scripts."	2006-05-09 2006-05-17	4.7	CVE-2006-2435 BUGTRAQ AIXAPAR OTHER-REF OTHER-REF FRSIRT SECUNIA
knowledgetree -- knowledgetree	The Debian package of knowledgetree 2.0.7 creates environment.php with world-readable permissions, which allows local users to obtain sensitive information such as the username and password for the KnowledgeTree database.	unknown 2006-05-18	5.6	CVE-2006-2443 DEBIAN
KPhone -- KPhone	kphone 4.2 creates .qt/kphonerc with world-readable permissions, which allows local users to read usernames and SIP passwords.	unknown 2006-05-18	5.6	CVE-2006-2442 DEBIAN
Limbo CMS -- Limbo CMS	SQL injection vulnerability in the weblinks option (weblinks.html.php) in Limbo CMS allows remote attackers to execute arbitrary SQL commands via the catid parameter.	2006-05-07 2006-05-15	4.7	CVE-2006-2363 BUGTRAQ OTHER-REF OTHER-REF SECUNIA
Macromedia -- ColdFusion	Cross-site scripting (XSS) vulnerability in the validation feature in Macromedia ColdFusion 5 and earlier allows remote attackers to inject arbitrary web script or HTML via a "_required" field when the associated normal field is missing or empty, which is not sanitized before being presented in an error message.	2006-05-10 2006-05-15	4.7	CVE-2006-2364 BUGTRAQ BID

Mozilla -- Bugzilla	Bugzilla 2.20rc1 through 2.20 and 2.21.1, when using RSS 1.0, allows remote attackers to conduct cross-site scripting (XSS) attacks via a title element with HTML encoded sequences such as ">", which are automatically decoded by some RSS readers. NOTE: this issue is not in Bugzilla itself, but rather due to design or documentation inconsistencies within RSS, or implementation vulnerabilities in RSS readers. While this issue normally would not be included in CVE, it is being identified since the Bugzilla developers have addressed it.	unknown 2006-05-16	4.7	CVE-2006-2420 BUGTRAQ OTHER-REF OTHER-REF OSVDB SECUNIA
MP3Info -- MP3Info	Buffer overflow in MP3Info 0.8.4 allows attackers to execute arbitrary code via a long command line argument. NOTE: if mp3info is not installed setuid or setgid in any reasonable context, then this issue might not be a vulnerability.	2006-05-14 2006-05-19	5.6	CVE-2006-2465 OTHER-REF BID SECTRACK
OZJournals -- OZJournals	Cross-site scripting (XSS) vulnerability in OZJournals 1.2 allows remote attackers to inject arbitrary web script or HTML via the vname parameter in the comments functionality.	2006-05-12 2006-05-15	4.7	CVE-2006-2390 OTHER-REF BID FRSIRT SECUNIA
PHP-Fusion -- PHP-Fusion	SQL injection vulnerability in messages.php in PHP-Fusion 6.00.307 and earlier allows remote authenticated users to execute arbitrary SQL commands via the srch_where parameter.	2006-05-17 2006-05-19	4.7	CVE-2006-2459 BUGTRAQ OTHER-REF FRSIRT SECUNIA
phpODP -- phpODP	Cross-site scripting (XSS) vulnerability in phpODP 1.5h allows remote attackers to inject arbitrary web script via the browse parameter.	2006-05-15 2006-05-15	4.7	CVE-2006-2396 OTHER-REF BID FRSIRT SECUNIA
Pixaria -- PopPhoto	PHP remote file inclusion vulnerability in resources/includes/popp.config.loader.inc.php in PopPhoto 3.5.4 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the include_path parameter (cfg['popphoto_base_path'] variable).	2006-05-14 2006-05-15	4.7	CVE-2006-2395 OTHER-REF FRSIRT SECUNIA BID OSVDB SECTRACK
RadScripts -- RadLance Gold	Directory traversal vulnerability in popup.php in RadScripts RadLance Gold 7.0 allows remote attackers to read arbitrary files via a .. (dot dot) in the read parameter.	unknown 2006-05-15	4.7	CVE-2006-2404 OTHER-REF BID OTHER-REF FRSIRT OSVDB SECUNIA
Raydium -- Raydium	Format string vulnerability in the raydium_console_line_add function in console.c in Raydium before SVN revision 310 allows local users to execute arbitrary code via format string specifiers in the format parameter.	unknown 2006-05-16	4.9	CVE-2006-2409 BUGTRAQ OTHER-REF OTHER-REF SECUNIA FRSIRT
SugarCRM -- SugarCRM	Sugar Suite Open Source (SugarCRM) 4.2 and earlier, when register_globals is enabled, does not protect critical variables such as $_GLOBALS and $_SESSION from modification, which allows remote attackers to conduct attacks such as directory traversal or PHP remote file inclusion, as demonstrated by modifying the GLOBALS[sugarEntry] parameter.	2006-05-15 2006-05-19	4.7	CVE-2006-2460 BUGTRAQ OTHER-REF BID FRSIRT SECTRACK SECUNIA
Sun -- JRE Sun -- SDK Sun -- JDK	Sun Java Runtime Environment (JRE) 1.5.0_6 and earlier, JDK 1.5.0_6 and earlier, and SDK 1.5.0_6 and earlier allows remote attackers to cause a denial of service (disk consumption) by using the Font.createFont function to create temporary files of arbitrary size in the %temp% directory.	2006-05-14 2006-05-17	5.2	CVE-2006-2426 BUGTRAQ OTHER-REF FRSIRT SECUNIA
Turnkey Web Tools -- PHP Live Helper	Cross-site scripting (XSS) vulnerability in chat.php in PHP Live Helper allows remote attackers to inject arbitrary web script or HTML via the PHPSESSID parameter.	2006-05-12 2006-05-15	4.7	CVE-2006-2394 BUGTRAQ BID
Vizra -- Vizra	Cross-site scripting (XSS) vulnerability in a_login.php in Vizra allows remote attackers to inject arbitrary web script or HTML via the message parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2006-05-11 2006-05-15	4.7	CVE-2006-2365 OTHER-REF BID

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
BEA Systems -- Weblogic Server	BEA WebLogic Server before 8.1 Service Pack 4 does not properly set the Quality of Service in certain circumstances, which prevents some transmissions from being encrypted via SSL, and allows remote attackers to more easily read potentially sensitive network traffic.	2006-05-16 2006-05-19	2.3	CVE-2006-2461 BEA FRSIRT SECTRACK SECUNIA
BEA Systems -- Weblogic Server	BEA WebLogic Server 8.1 before Service Pack 4 and 7.0 before Service Pack 6, may send sensitive data over non-secure channels when using JTA transactions, which allows remote attackers to read potentially sensitive network traffic.	2006-05-15 2006-05-19	2.3	CVE-2006-2462 BEA FRSIRT SECTRACK SECUNIA
BEA Systems -- Weblogic Server	BEA WebLogic Server 8.1 up to SP4 and 7.0 up to SP6 allows remote attackers to obtain the source code of JSP pages during certain circumstances related to a "timing window" when a compilation error occurs, aka the "JSP showcode vulnerability."	unknown 2006-05-19	1.9	CVE-2006-2466 BEA FRSIRT SECUNIA
BEA Systems -- Weblogic Server	BEA WebLogic Server 8.1 up to SP4, 7.0 up to SP6, and 6.1 up to SP7 displays the internal IP address of the WebLogic server in the WebLogic Server Administration Console, which allows remote authenticated administrators to determine the address.	2006-05-16 2006-05-19	1.4	CVE-2006-2467 BEA FRSIRT SECUNIA
BEA Systems -- Weblogic Server	The WebLogic Server Administration Console in BEA WebLogic Server 8.1 up to SP4 and 7.0 up to SP6 displays the domain name in the Console login form, which allows remote attackers to obtain sensitive information.	2006-05-16 2006-05-19	1.4	CVE-2006-2468 BEA FRSIRT SECUNIA
BEA Systems -- Weblogic Server BEA Systems -- WebLogic Express	Multiple vulnerabilities in BEA WebLogic Server 8.1 through SP4, 7.0 through SP6, and 6.1 through SP7 leak sensitive information to remote attackers, including (1) DNS and IP addresses to address to T3 clients, (2) internal sensitive information using GetIORServlet, (3) certain "server details" in exceptions when invalid XML is provided, and (4) a stack trace in a SOAP fault.	unknown 2006-05-19	2.3	CVE-2006-2471 BEA FRSIRT SECUNIA
BEA Systems -- Weblogic Server BEA Systems -- WebLogic Express	Unspecified vulnerability in BEA WebLogic Server 9.1 and 9.0, 8.1 through SP5, 7.0 through SP6, and 6.1 through SP7 allows untrusted applications to obtain private server keys.	unknown 2006-05-19	2.3	CVE-2006-2472 BEA FRSIRT SECUNIA
Bitrix -- Bitrix Site Manager	Bitrix Site Manager 4.1.x stores updater.log under the web document root with insufficient access control, which allows remote attackers to obtain sensitive information.	2006-05-18 2006-05-19	2.3	CVE-2006-2476 BUGTRAQ FRSIRT SECTRACK SECUNIA
Bitrix -- Bitrix Site Manager	Cross-site scripting (XSS) vulnerability in the administrative interface Bitrix Site Manager 4.1.x allows remote attackers to inject arbitrary web script or HTML via unspecified inputs.	2006-05-18 2006-05-19	2.8	CVE-2006-2477 BUGTRAQ FRSIRT SECTRACK SECUNIA
Bitrix -- Bitrix Site Manager	Bitrix Site Manager 4.1.x allows remote attackers to redirect users to other websites via a modified back_url during a HTTP POST request. NOTE: this issue has been referred to as "cross-site scripting," but that is inconsistent with the common use of the term.	2006-05-18 2006-05-19	2.3	CVE-2006-2478 BUGTRAQ FRSIRT SECTRACK SECUNIA
Bitrix -- Bitrix Site Manager	The Update functionality in Bitrix Site Manager 4.1.x does not verify the authenticity of downloaded updates, which allows remote attackers to obtain sensitive information and ultimately execute arbitrary PHP code via DNS cache poisoning that redirects the user to a malicious site.	2006-05-18 2006-05-19	2.3	CVE-2006-2479 BUGTRAQ FRSIRT SECTRACK
Caucho Technology -- Resin	Directory traversal vulnerability in Caucho Resin 3.0.17 and 3.0.18 for Windows allows remote attackers to read arbitrary files via a "C:%5C" (encoded drive letter) in a URL.	unknown 2006-05-17	3.3	CVE-2006-1953 BUGTRAQ BID FRSIRT VULNWATCH OTHER-REF
Caucho Technology -- Resin	The viewfile servlet in the documentation package (resin-doc) for Caucho Resin 3.0.17 and 3.0.18 allows remote attackers to obtain the source code for file under the web root via the file parameter.	2006-05-05 2006-05-17	2.3	CVE-2006-2437 BUGTRAQ BID FRSIRT
Caucho Technology -- Resin	Directory traversal vulnerability in the viewfile servlet in the documentation package (resin-doc) for Caucho Resin 3.0.17 and 3.0.18 allows remote attackers to read arbitrary files under other web roots via the contextpath parameter. NOTE: this issue can produce resultant path disclosure when the	unknown 2006-05-17	2.3	CVE-2006-2438 BUGTRAQ BID FRSIRT

	parameter is invalid.			
Clansys -- Clansys	Cross-site scripting (XSS) vulnerability in index.php in Clansys (aka Clanpage System) 1.0 and 1.1 allows remote attackers to inject arbitrary web script or HTML via the func parameter in a search function.	unknown 2006-05-15	2.3	CVE-2006-2367 BUGTRAQ OTHER-REF SECTRACK SECUNIA XF
Cosmoshop -- Cosmoshop	Directory traversal vulnerability in (1) edit_mailtexte.cgi and (2) bestmail.cgi in Cosmoshop 8.11.106 and earlier allows remote administrators to read arbitrary files via ".." sequences in the file parameter.	2006-05-18 2006-05-19	3.3	CVE-2006-2475 BUGTRAQ
Dovecot -- Dovecot	Directory traversal vulnerability in Dovecot 1.0 beta and 1.0 allows remote attackers to list files and directories under the mbox parent directory and obtain mailbox names via ".." sequences in the (1) LIST or (2) DELETE IMAP command.	unknown 2006-05-16	2.3	CVE-2006-2414 BUGTRAQ OTHER-REF OTHER-REF BID
Empire Server -- Empire Server	The client_cmd function in Empire 4.3.2 and earlier allows remote attackers to cause a denial of service (application crash) by causing long text strings to be appended to the player->client buffer, which causes an invalid memory access.	2006-05-12 2006-05-15	2.3	CVE-2006-2393 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECUNIA
GNUnet -- GNUnet	GNUnet before SVN revision 2781 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via an empty UDP datagram, possibly involving FIONREAD errors.	unknown 2006-05-16	2.3	CVE-2006-2413 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECUNIA
GPhotos -- GPhotos	Directory traversal vulnerability in index.php in GPhotos 1.5 and earlier allows remote attackers to read arbitrary files via the rep parameter.	2006-05-13 2006-05-15	2.3	CVE-2006-2398 BUGTRAQ BID FRSIRT SECUNIA OSVDB
IBM -- Websphere	Unspecified vulnerability in WebSphere 5.1.1 (or any earlier cumulative fix) Common Configuration Mode + CommonArchive and J2EE Models might allow attackers to obtain sensitive information via the trace.	2006-05-09 2006-05-17	2.3	CVE-2006-2434 BUGTRAQ OTHER-REF FRSIRT SECUNIA
IPswitch -- WhatsUp Professional	Multiple cross-site scripting (XSS) vulnerabilities in IPswitch WhatsUp Professional 2006 and WhatsUp Professional 2006 Premium allow remote attackers to inject arbitrary web script or HTML via the (1) sDeviceView or (2) nDeviceID parameter to (a) NmConsole/Navigation.asp or (3) sHostname parameter to (b) NmConsole/ToolResults.asp.	2006-05-11 2006-05-15	2.3	CVE-2006-2351 BUGTRAQ BID FRSIRT SECUNIA
Ipswitch -- WhatsUp Professional	NmConsole/DeviceSelection.asp in Ipswitch WhatsUp Professional 2006 and WhatsUp Professional 2006 Premium allows remote attackers to redirect users to other websites via the (1) sCancelURL and possibly (2) sRedirectUrl parameters.	2006-05-11 2006-05-15	2.3	CVE-2006-2353 BUGTRAQ FRSIRT SECUNIA
Ipswitch -- WhatsUp Professional	Ipswitch WhatsUp Professional 2006 and WhatsUp Professional 2006 Premium allows remote attackers to obtain source code for scripts via a trailing dot in a request to NmConsole/Login.asp.	unknown 2006-05-15	2.3	CVE-2006-2357 BUGTRAQ FRSIRT SECUNIA
libextractor -- libextractor	Multiple heap-based buffer overflows in Libextractor 0.5.13 and earlier allow remote attackers to execute arbitrary code via (1) the asf_read_header function in the ASF plugin (plugins/asfextractor.c), and (2) the parse_trak_atom function in the QT plugin (plugins/qtextractor.c).	2006-05-17 2006-05-18	3.7	CVE-2006-2458 BUGTRAQ BID FRSIRT SECTRACK SECUNIA OTHER-REF
Linux -- Linux kernel	Linux kernel before 2.6.13 allows local users to cause a denial of service (crash) via a dio transfer from the sg driver to memory mapped (mmap) IO space.	unknown 2006-05-18	2.3	CVE-2006-1528 OTHER-REF OTHER-REF OTHER-REF
Linux -- Linux kernel	choose_new_parent in Linux kernel before 2.6.11.12 includes certain debugging code, which allows local users to cause a denial of service (panic) by causing certain circumstances involving termination of a parent process.	unknown 2006-05-18	2.5	CVE-2006-1855 OTHER-REF

OpenOBEX -- OpenOBEX	ircp_io.c in libopenobex for ircp 1.2, when ircp is run with the -r option, does not prompt the user when overwriting files, which allows user-complicit remote attackers to overwrite dangerous files via an arbitrary destination file name in an OBEX File Transfer session.	unknown 2006-05-15	1.9	CVE-2006-2366 OTHER-REF BID
OpenWiki -- OpenWiki	Cross-site scripting (XSS) vulnerability in ow.asp in OpenWiki 0.78 allows remote attackers to inject arbitrary web script or HTML via the p parameter.	2006-05-17 2006-05-19	2.3	CVE-2006-2473 BUGTRAQ
Outgun -- Outgun	The leetnet functions (leetnet/rudp.cpp) in Outgun 1.0.3 bot 2 and earlier allow remote attackers to cause a denial of service (game interruption) via large packets, which cause an exception to be thrown.	2006-05-12 2006-05-15	3.3	CVE-2006-2400 BUGTRAQ ALTERVISTA BID FRSIRT SECUNIA
Outgun -- Outgun	The leetnet functions (leetnet/rudp.cpp) in Outgun 1.0.3 bot 2 and earlier allow remote attackers to cause a denial of service (application crash) via packets with incorrect message sizes, which triggers a buffer over-read.	2006-05-12 2006-05-15	3.3	CVE-2006-2401 BUGTRAQ ALTERVISTA BID FRSIRT SECUNIA
Outgun -- Outgun	Buffer overflow in the changeRegistration function in servernet.cpp for Outgun 1.0.3 bot 2 and earlier allows remote attackers to change the registration information of other players via a long string.	2006-05-12 2006-05-15	2.3	CVE-2006-2402 BUGTRAQ ALTERVISTA BID FRSIRT SECUNIA
PHP -- Directory Listing Script	Cross-site scripting (XSS) vulnerability in index.php in Directory Listing Script allows remote attackers to inject arbitrary web script or HTML via the dir parameter.	unknown 2006-05-16	2.3	CVE-2006-2419 ALTERVISTA FRSIRT SECUNIA
phpBB Group -- phpBB	Cross-site scripting (XSS) vulnerability in charts.php in the Chart mod for phpBB allows remote attackers to inject arbitrary web script or HTML via the id parameter. NOTE: this issue might be resultant from SQL injection.	unknown 2006-05-15	2.3	CVE-2006-2359 BUGTRAQ BUGTRAQ BID
phpCOIN -- phpCOIN	phpCOIN 1.2.3 and earlier stores messages based upon e-mail addresses, which allows remote authenticated users to read messages for other users by adding the sender's e-mail address as an "additional contact".	unknown 2006-05-17	2.3	CVE-2006-2422 OTHER-REF BID FRSIRT SECUNIA
phpMyAdmin -- phpMyAdmin	Cross-site scripting (XSS) vulnerability in phpMyAdmin 2.8.0.x before 2.8.0.4 allows remote attackers to inject arbitrary web script or HTML via the theme parameter in unknown scripts. NOTE: the lang parameter is already covered by CVE-2006-2031.	unknown 2006-05-16	2.3	CVE-2006-2417 OTHER-REF FRSIRT SECUNIA BID
phpMyAdmin -- phpMyAdmin	Cross-site scripting (XSS) vulnerabilities in certain versions of phpMyAdmin before 2.8.0.4 allow remote attackers to inject arbitrary web script or HTML via the db parameter in unknown scripts.	unknown 2006-05-16	3.3	CVE-2006-2418 PHPMYADMIN FRSIRT SECUNIA BID
phpRemoteView -- phpRemoteView	Multiple cross-site scripting (XSS) vulnerabilities in PRV.php in PhpRemoteView, possibly 2003-10-23 and earlier, allow remote attackers to inject arbitrary web script or HTML via the (1) f, (2) d, and (3) ref parameters, and the (4) "MAKE DIR" and (5) "Full file name" fields.	2006-05-16 2006-05-17	2.3	CVE-2006-2425 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Pioneers -- Pioneers meta-server	Pioneers meta-server before 0.9.55, when the server-console is not installed, allows remote attackers to cause a denial of service (crash) via certain requests from an older gnocatan client to create a new game.	unknown 2006-05-18	2.3	CVE-2006-2441 SOURCEFORGE DEBIAN
Raydium -- Raydium	raydium_network_netcall_exec function in network.c in Raydium SVN revision 312 and earlier allows remote attackers to cause a denial of service (application crash) via a packet of type 0xFF, which causes a null dereference.	unknown 2006-05-16	2.3	CVE-2006-2410 BUGTRAQ OTHER-REF SECUNIA FRSIRT
Raydium -- Raydium	The raydium_network_read function in network.c in Raydium SVN revision 312 and earlier allows remote attackers to cause a denial of service (application crash) via a large ID, which causes an invalid memory access (buffer over-read).	unknown 2006-05-16	2.3	CVE-2006-2412 BUGTRAQ OTHER-REF SECUNIA FRSIRT

SelectaPix -- SelectaPix	view_album.php in SelectaPix 1.31 and earlier allows remote attackers to obtain the installation path via a certain request, which displays the path in an error message, possibly due to an invalid or missing parameter.	2006-05-14 2006-05-19	2.3	CVE-2006-2463 SECTRACK
Skype Technologies -- Skype	Unspecified vulnerability in the URI handler in Skype 2.0.*.104 and 2.5.*.0 through 2.5.*.78 for Windows allows remote authorized attackers to download arbitrary files via a crafted URL.	unknown 2006-05-19	1.9	CVE-2006-2312 OTHER-REF BID SECUNIA
SWSoft -- Confixx	Cross-site scripting (XSS) vulnerability in ftplogin/index.php in Confixx 3.1.2 allows remote attackers to inject arbitrary web script or HTML via the login parameter.	2006-05-15 2006-05-17	2.3	CVE-2006-2423 BUGTRAQ FRSIRT SECUNIA BID
Unclassified NewsBoard -- Unclassified NewsBoard	Directory traversal vulnerability in unb_lib/abbc.conf.php in Unclassified NewsBoard (UNB) 1.6.1 patch 1 and earlier, when register_globals is enabled, allows remote attackers to include arbitrary files via .. (dot dot) sequences and a trailing null byte (%00) in the ABBC[Config][smileset] parameter to unb_lib/abbc.css.php.	2006-05-11 2006-05-16	2.7	CVE-2006-2405 BUGTRAQ ALTERVISTA OTHER-REF BID FRSIRT SECUNIA
Unclassified NewsBoard -- Unclassified NewsBoard	Directory traversal vulnerability in bb_lib/abbc.css.php in Unclassified NewsBoard (UNB) 1.5.3-d and possibly earlier versions, when register_globals is enabled, allows remote attackers to include arbitrary files via .. (dot dot) sequences and a trailing null byte (%00) in the design_path parameter. NOTE: this is closely related, but a different vulnerability than the ABBC[Config][smileset] parameter.	unknown 2006-05-16	1.9	CVE-2006-2406 OTHER-REF
Web-Labs -- Web-Labs CMS	Multiple cross-site scripting (XSS) vulnerabilities in various scripts in Web-Labs CMS allow remote attackers to inject arbitrary web script or HTML via (1) the search parameter and (2) unspecified fields related to e-mail alerts. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-05-15	2.3	CVE-2006-2358 BID FRSIRT SECUNIA

Back to top

Last updated May 22, 2006