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
2X -- ThinClientServer	Directory traversal vulnerability in 2X TFTP service (TFTPd.exe) 3.2.0.0 and earlier in 2X ThinClientServer 5.0_sp1-r3497 and earlier allows remote attackers to read or overwrite arbitrary files via a ... (dot dot dot) in the filename.	unknown 2008-04-02	7.5	CVE-2008-1620 OTHER-REF OTHER-REF FRSIRT SECUNIA

Adobe -- Flash	Interaction error between Adobe Flash and multiple Universal Plug and Play (UPnP) services allow remote attackers to perform Cross-Site Request Forgery (CSRF) style attacks by using the Flash navigateToURL function to send a SOAP message to a UPnP control point, as demonstrated by changing the primary DNS server.	unknown 2008-04-02	9.3	CVE-2008-1654 BUGTRAQ FULLDISC OTHER-REF CERT-VN
Apache-SSL -- Apache-SSL	The ExpandCert function in Apache-SSL before apache_1.3.41+ssl_1.59 does not properly handle (1) '/' and (2) '=' characters in a Distinguished Name (DN) in a client certificate, which might allow remote attackers to bypass authentication via a crafted DN that triggers overwriting of environment variables.	unknown 2008-04-03	7.5	CVE-2008-0555 BUGTRAQ OTHER-REF OTHER-REF BID
Apple -- Quicktime	Heap-based buffer overflow in quickTime.qts in Apple QuickTime before 7.4.5 allows remote attackers to execute arbitrary code via a crafted PICT image file, related to an improperly terminated memory copy loop.	unknown 2008-04-04	8.3	CVE-2008-1019 OTHER-REF OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF

Apple -- CUPS	Buffer overflow in the gif_read_lzw in CUPS 1.3.6 allows remote attackers to have an unknown impact via a GIF file with a large code_size value, a similar issue to CVE-2006-4484.	unknown 2008-04-03	7.5	CVE-2008-1373 OTHER-REF GENTOO REDHAT REDHAT BID FRSIRT SECTRACK SECUNIA
Arnos Toolbox -- WP-Download	SQL injection vulnerability in wp-download.php in the WP-Download 1.2 plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the dl_id parameter.	unknown 2008-04-02	7.5	CVE-2008-1646 MILW0RM BID SECUNIA
Chilkat Software -- ChilkatHttp ActiveX	The ChilkatHttp. ChilkatHttp.1 and ChilkatHttp. ChilkatHttpRequest.1 ActiveX controls in ChilkatHttp.dll 2.4.0.0, 2.3.0.0, and earlier in ChilkatHttp ActiveX expose the unsafe SaveLastError method, which allows remote attackers to overwrite arbitrary files. NOTE: some of these details are obtained from third party information.	unknown 2008-04-02	7.5	CVE-2008-1647 OTHER-REF FRSIRT SECUNIA

Clever Copy -- Clever Copy	SQL injection vulnerability in postview.php in Clever Copy 3.0 allows remote attackers to execute arbitrary SQL commands via the ID parameter, a different vector than CVE-2008-0363 and CVE-2006-0583. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-01	7.5	CVE-2008-1608 OTHER-REF BID XF
comix -- comix	comix 3.6.4 allows attackers to execute arbitrary commands via a filename containing shell metacharacters that are not properly sanitized when executing the rar, unrar, or jpegtran programs.	unknown 2008-03-31	7.5	CVE-2008-1568 OTHER-REF
Compaq -- Presario C700 HP -- G7000 Compaq -- Presario A900 HP -- hpqflash_for_hp_notebook_system_bios	Unspecified vulnerability in the BIOS F.26 and earlier for the HP Compaq Notebook PC allows physically proximate attackers to obtain privileged access via unspecified vectors, possibly involving an authentication bypass of the power-on password.	unknown 2008-03-31	7.2	CVE-2008-0706 HP BID SECTRACK
EfesTech -- Video	SQL injection vulnerability in default.asp in EfesTECH Video 5.0 allows remote attackers to execute arbitrary SQL commands via the catID parameter.	unknown 2008-04-02	7.5	CVE-2008-1641 BUGTRAQ BID SECUNIA XF

eggblog -- eggblog	SQL injection vulnerability in eggBlog before 4.0.1 allows remote attackers to execute arbitrary SQL commands via an unspecified cookie. NOTE: this might overlap CVE-2008-0159.	unknown 2008-04-02	7.5	CVE-2008-1626 OTHER-REF OTHER-REF BID SECUNIA XF
EMEDIA OFFICE GmbH -- CuteFlow	Multiple cross-site scripting (XSS) vulnerabilities in CuteFlow 1.5.0 and 2.10.0 allow remote attackers to inject arbitrary web script or HTML via the language parameter to (1) page/showcirculation.php; and (2) edittemplate_step2.php, (3) showfields.php, (4) showuser.php, (5) editmailinglist_step1.php, and (6) showtemplates.php in pages/.	unknown 2008-04-02	7.5	CVE-2008-1630 BUGTRAQ BID SECUNIA
EMEDIA OFFICE GmbH -- CuteFlow	SQL injection vulnerability in login.php in CuteFlow 1.5.0 and 2.10.0 allows remote attackers to execute arbitrary SQL commands via the UserId parameter, related to the login form field in index.php.	unknown 2008-04-02	7.5	CVE-2008-1631 BUGTRAQ SECUNIA

EMEDIA OFFICE GmbH -- CuteFlow	Multiple SQL injection vulnerabilities in CuteFlow 2.10.0 allow remote authenticated users to execute arbitrary SQL commands via the (1) listid parameter to pages/editmailinglist_step1.php, the (2) userid parameter to pages/edituser.php, the (3) fieldid parameter to pages/editfield.php, and the (4) templateid to pages/edittemplate_step1.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-02	7.5	CVE-2008-1632 SECUNIA
Francisco Burzi -- PHP-Nuke	PHP-Nuke Platinum 7.6.b.5 allows remote attackers to obtain configuration information via a direct request to maintenance/index.php, which reveals settings such as magic_quotes_gpc.	unknown 2008-04-03	7.5	CVE-2008-1680 MILW0RM
Guillaume Meister -- PHP SpamManager	Directory traversal vulnerability in body.php in phpSpamManager (phpSM) 0.53 beta allows remote attackers to read arbitrary local files via a .. (dot dot) in the filename parameter.	unknown 2008-04-02	7.5	CVE-2008-1645 MILW0RM BID FRSIRT

Hotscripts -- pjirc phpBB -- pjirc_module	Directory traversal vulnerability in forum/irc/irc.php in the PJIRC 0.5 module for phpBB allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the phpEx parameter.	unknown 2008-03-31	7.5	CVE-2008-1565 BUGTRAQ BID XF
IBM -- AIX	The checkpoint and restart feature in the kernel in IBM AIX 5.2, 5.3, and 6.1 does not properly protect kernel memory, which allows local users to read and modify portions of memory and gain privileges via unspecified vectors involving a restart of a 64-bit process, probably related to the as_getadsp64 function.	unknown 2008-03-31	7.2	CVE-2008-1593 OTHER-REF OTHER-REF OTHER-REF AIXAPAR AIXAPAR AIXAPAR AIXAPAR BID FRSIRT SECTRACK
IBM -- AIX	Trusted Execution in IBM AIX 6.1 uses an incorrect pathname argument in a call to the trustchk_block_write function, which might allow local users to modify trusted files, related to missing checks in the TSD_FILES_LOCK policy for modifications performed via hard links, a different vulnerability than CVE-2007-6680.	unknown 2008-03-31	7.2	CVE-2008-1596 OTHER-REF OTHER-REF OTHER-REF AIXAPAR BID FRSIRT SECTRACK

IBM -- AIX	The nddstat programs on IBM AIX 5.2, 5.3, and 6.1 do not properly handle environment variables, which allows local users to gain privileges by invoking (1) atmstat, (2) entstat, (3) fddistat, (4) hdlcstat, or (5) tokstat.	unknown 2008-03-31	7.2	CVE-2008-1599 OTHER-REF OTHER-REF OTHER-REF AIXAPAR AIXAPAR AIXAPAR AIXAPAR FRSIRT SECTRACK
IBM -- AIX	The lsmcode program on IBM AIX 5.2, 5.3, and 6.1 does not properly handle environment variables, which allows local users to gain privileges, a different vulnerability than CVE-2004-1329.	unknown 2008-03-31	7.2	CVE-2008-1600 OTHER-REF OTHER-REF OTHER-REF AIXAPAR AIXAPAR AIXAPAR AIXAPAR FRSIRT SECTRACK
IBM -- AIX	Stack-based buffer overflow in the reboot program on IBM AIX 5.2 and 5.3 allows local users in the shutdown group to gain privileges.	unknown 2008-03-31	7.2	CVE-2008-1601 OTHER-REF OTHER-REF OTHER-REF AIXAPAR AIXAPAR

				FRSIRT SECTRACK
JGS-XA -- JGS_Treffen	SQL injection vulnerability in jgs_treffen.php in the JGS-XA JGS-Treffen 2.0.2 and earlier addon for Woltlab Burning Board (wBB) allows remote attackers to execute arbitrary SQL commands via the view_id parameter in an ansicht action.	unknown 2008-04-02	7.5	CVE-2008-1640 MILW0RM BID FRSIRT
LANDesk Software -- LANDesk Management Suite	Directory traversal vulnerability in the PXE TFTP Service (PXEMTFTP.exe) in LANDesk Management Suite (LDMS) 8.7 SP5 and earlier and 8.8 allows remote attackers to read arbitrary files via unspecified vectors.	unknown 2008-04-02	7.5	CVE-2008-1643 OTHER-REF BID FRSIRT SECUNIA
Leadtools -- multimedia_toolkit	The (1) ltmmCaptureCtrl Class, (2) ltmmConvertCtrl Class, and (3) ltmmPlayCtrl Class ActiveX controls (ltmm15.dll 15.1.0.17 and earlier) in LEADTOOLS Multimedia Toolkit 15 allow attackers to overwrite arbitrary files via the SaveSettingsToFile method.	unknown 2008-04-01	7.5	CVE-2008-1605 OTHER-REF OTHER-REF BID SECUNIA XF

Lotus Web Studios Inc -- Smoothflash	SQL injection vulnerability in admin_view_image.php in Smoothflash allows remote attackers to execute arbitrary SQL commands via the cid parameter.	unknown 2008-04-02	9.4	CVE-2008-1623 MILW0RM SECUNIA
Macrovision -- InstallShield	The Macrovision InstallShield InstallScript One-Click Install (OCI) ActiveX control 12.0 before SP2 does not validate the DLL files that are named as parameters to the control, which allows remote attackers to download arbitrary library code onto a client machine.	unknown 2008-04-03	9.3	CVE-2007-5661 IDEFENSE OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
MPlayer -- MPlayer	Uncontrolled array index in the sdpplin_parse function in stream/realrtsp/sdpplin.c in MPlayer 1.0 rc2 allows remote attackers to overwrite memory and execute arbitrary code via a large streamid SDP parameter. NOTE: this issue has been referred to as an integer overflow.	unknown 2008-03-31	10.0	CVE-2008-1558 MILW0RM FRSIRT SECUNIA

MyioSoft -- EasyNews	SQL injection vulnerability in dynamicpages/index.php in EasyNews 4.0 allows remote attackers to execute arbitrary SQL commands via the read parameter in an edp_Help_Internal_News action.	unknown 2008-04-02	7.5	CVE-2008-1650 BUGTRAQ MILW0RM
MyioSoft -- EasyNews	Directory traversal vulnerability in admin/login.php in EasyNews 4.0 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang parameter.	unknown 2008-04-02	7.5	CVE-2008-1651 BUGTRAQ MILW0RM
Neat -- Weblog	SQL injection vulnerability in index.php in Neat weblog 0.2 allows remote attackers to execute arbitrary SQL commands via the articleId parameter in a show action, probably related to the showArticle function in lib/lib_article.include.php.	unknown 2008-04-02	7.5	CVE-2008-1639 MILW0RM BID FRSIRT
OTRS -- OTRS	The SOAP interface in OTRS 2.1.x before 2.1.8 and 2.2.x before 2.2.6 does not perform any "security checks," which allows remote attackers to "read and modify objects" via SOAP requests.	unknown 2008-04-01	7.5	CVE-2008-1515 OTHER-REF

perlbal -- perlbal	Directory traversal vulnerability in the _serve_request_multiple function in lib/Perlbal/ClientHTTPBase.pm in Perlbal before 1.70, when concat get is enabled, allows remote attackers to read arbitrary files in a parent directory via a directory traversal sequence in an unspecified parameter. NOTE: some of these details are obtained from third party information.	unknown 2008-04-02	7.5	CVE-2008-1652 OTHER-REF FRSIRT SECUNIA XF
PostNuke Software Foundation -- PostNuke	The pnVarPrepForStore function in PostNuke 0.764 and earlier skips input sanitization when magic_quotes_runtime is enabled, which allows remote attackers to conduct SQL injection attacks and execute arbitrary SQL commands via input associated with server variables, as demonstrated by the CLIENT_IP HTTP header (HTTP_CLIENT_IP variable).	unknown 2008-03-31	7.5	CVE-2008-1591 MILW0RM BID XF

Raven PHP Scripts -- Keep It Simple Guest Book	Directory traversal vulnerability in view_private.php in Keep It Simple Guest Book (KISGB) 5.0.0 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the tmp_theme parameter. NOTE: 5.1.1 is also reportedly affected.	unknown 2008-04-02	7.5	CVE-2008-1635 MILW0RM XF
RunCMS -- photo_module RunCMS -- RunCMS	SQL injection vulnerability in viewcat.php in the Photo 3.02 module for RunCMS allows remote attackers to execute arbitrary SQL commands via the cid parameter.	unknown 2008-03-31	7.5	CVE-2008-1551 MILW0RM BID SECUNIA XF
Savas Place -- Savas Guestbook	Directory traversal vulnerability in index.php in Sava's GuestBook 2.0 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the action parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-02	7.5	CVE-2008-1642 BID SECUNIA

Savas Place -- Savas Link Manager	SQL injection vulnerability in viewlinks.php in Sava's Link Manager 2.0 allows remote attackers to execute arbitrary SQL commands via the category parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-02	7.5	CVE-2008-1644 BID SECUNIA
Savas Place -- Savas Link Manager	Directory traversal vulnerability in index.php in Sava's Link Manager 2.0 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the q parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-02	7.5	CVE-2008-1653 BID SECUNIA
Sympa -- Sympa	Sympa before 5.4 allows remote attackers to cause a denial of service (daemon crash) via an e-mail message with a malformed value of the Content-Type header and unspecified other headers. NOTE: some of these details are obtained from third party information.	unknown 2008-04-02	7.5	CVE-2008-1648 OTHER-REF OTHER-REF SECUNIA

tallsoft_quick -- tftp_server_pro	Stack-based buffer overflow in TallSoft Quick TFTP Server Pro 2.1 allows remote attackers to cause a denial of service or execute arbitrary code via a long mode field in a read or write request.	unknown 2008-04-01	7.5	CVE-2008-1610 MILW0RM OTHER-REF BID SECUNIA
tftp-server -- winagents_tftp_server	Stack-based buffer overflow in TFTP Server SP 1.4 for Windows allows remote attackers to cause a denial of service or execute arbitrary code via a long filename in a read or write request.	unknown 2008-04-01	10.0	CVE-2008-1611 MILW0RM OTHER-REF SECUNIA
Whorl Ltd -- JShop Server	Directory traversal vulnerability in v2demo/page.php in Jshop Server 1.x through 2.x allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the xPage parameter.	unknown 2008-04-02	7.5	CVE-2008-1624 MILW0RM BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Alcatel-Lucent -- OmniPCX Office	Unspecified vulnerability in OmniPCX Office with Internet Access services OXO210 before 210/091.001, OXO600 before 610/014.001, and other versions, allows remote attackers to obtain OXO resources via an unspecified CGI script.	unknown 2008-04-02	6.8	CVE-2008-1331 OTHER-REF FRSIRT XF

Apple -- Quicktime	Apple QuickTime before 7.4.5 enables deserialization of QTJava objects by untrusted Java applets, which allows remote attackers to execute arbitrary code via a crafted applet.	unknown 2008-04-04	6.8	CVE-2008-1013 OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF
Apple -- Quicktime	Apple QuickTime before 7.4.5 does not properly handle external URLs in movies, which allows remote attackers to obtain sensitive information.	unknown 2008-04-04	5.8	CVE-2008-1014 OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF
Apple -- Quicktime	Buffer overflow in the data reference atom handling in Apple QuickTime before 7.4.5 allows remote attackers to execute arbitrary code via a crafted movie.	unknown 2008-04-04	6.8	CVE-2008-1015 OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF

Apple -- Quicktime	Apple QuickTime before 7.4.5 does not properly handle movie media tracks, which allows remote attackers to execute arbitrary code via a crafted movie that triggers memory corruption.	unknown 2008-04-04	6.8	CVE-2008-1016 OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF
Apple -- Quicktime	Heap-based buffer overflow in clipping region (aka crgn) atom handling in quicktime.qts in Apple QuickTime before 7.4.5 allows remote attackers to execute arbitrary code via a crafted movie.	unknown 2008-04-04	6.8	CVE-2008-1017 OTHER-REF OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF
Apple -- Quicktime	Heap-based buffer overflow in Apple QuickTime before 7.4.5 allows remote attackers to execute arbitrary code via an MP4A movie with a malformed Channel Compositor (aka chan) atom.	unknown 2008-04-04	6.8	CVE-2008-1018 OTHER-REF OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF

Apple -- Quicktime	Heap-based buffer overflow in quickTime.qts in Apple QuickTime before 7.4.5 on Windows allows remote attackers to execute arbitrary code via a crafted PICT image file with Kodak encoding, related to error checking and error messages.	unknown 2008-04-04	6.8	CVE-2008-1020 OTHER-REF OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF
Apple -- Quicktime	Heap-based buffer overflow in Animation codec content handling in Apple QuickTime before 7.4.5 on Windows allows remote attackers to execute arbitrary code via a crafted movie with run length encoding.	unknown 2008-04-04	6.8	CVE-2008-1021 OTHER-REF OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF
Apple -- Quicktime	Stack-based buffer overflow in Apple QuickTime before 7.4.5 allows remote attackers to execute arbitrary code via a crafted VR movie with an obji atom of zero size.	unknown 2008-04-04	6.8	CVE-2008-1022 OTHER-REF OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF

Apple -- Quicktime	Heap-based buffer overflow in Clip opcode parsing in Apple QuickTime before 7.4.5 on Windows allows remote attackers to execute arbitrary code via a crafted PICT image file.	unknown 2008-04-04	6.8	CVE-2008-1023 OTHER-REF CERT BID FRSIRT SECTRACK SECUNIA XF
Avast -- Avast Antivirus Professional Avast -- Avast Antivirus Home	aavmker4.sys in avast! Home and Professional 4.7 for Windows does not properly validate input to IOCTL 0xb2d60030, which allows local users to gain privileges via certain IOCTL requests.	unknown 2008-04-02	6.6	CVE-2008-1625 OTHER-REF OTHER-REF BID FRSIRT SECUNIA
BolinOS -- BolinOS	Directory traversal vulnerability in system/_b/contentFiles/gbincluder.php in BolinOS 4.6.1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the _bFileToInclude parameter.	unknown 2008-03-31	6.8	CVE-2008-1555 BUGTRAQ MILW0RM BID SECUNIA XF
BolinOS -- BolinOS	Multiple cross-site scripting (XSS) vulnerabilities in BolinOS 4.6.1 allow remote attackers to inject arbitrary web script or HTML via the (1) url parameter to (a) system/actionspages/_b/contentFiles/gBImageViewer.php, (2) ForEditor parameter to (b) system/actionspages/_b/contentFiles/gBselectorContents.php, (3) the PATH_INFO to (c) gBLoginPage.php and (d) gBPassword.php in system/actionspages/_b/contentFiles/, (4) formlogin parameter to system/actionspages/_b/contentFiles/gBLoginPage.php, and the (5) bolini_searchengine46Search parameter to (e) help/index.php.	unknown 2008-03-31	4.3	CVE-2008-1556 BUGTRAQ MILW0RM BID SECUNIA XF

BolinOS -- BolinOS	BolinOS 4.6.1 allows remote attackers to obtain sensitive information via a direct request to system/actionspages/_b/contentFiles/gBphpInfo.php, which calls the phpinfo function.	unknown 2008-03-31	5.0	CVE-2008-1557 BUGTRAQ MILW0RM SECUNIA XF
CDS Software Consortium -- Invenio	CDS Invenio 0.92.1 and earlier allows remote authenticated users to delete email notification alerts of arbitrary users via a modified internal UID.	unknown 2008-04-02	5.1	CVE-2008-1627 OTHER-REF OTHER-REF SECUNIA
Compaq -- 8510 Series BIOS Compaq -- 6515 Series BIOS Compaq -- 2510 Series BIOS Compaq -- 2210 Series BIOS Compaq -- 6910 Series BIOS Compaq -- 6715 Series BIOS Compaq -- 8710 Series BIOS Compaq -- 6510 Series BIOS Compaq -- 6710 Series BIOS Compaq -- 6720 Series BIOS Compaq -- 6820 Series BIOS Compaq -- 2710 Series BIOS Compaq -- 6520 Series BIOS	Unspecified vulnerability in the BIOS F.04 through F.11 for the HP Compaq Business Notebook PC allows local users to cause a denial of service via unspecified vectors.	unknown 2008-03-31	4.9	CVE-2008-0211 HP BID SECTRACK

cubecart -- cubecart	Multiple cross-site scripting (XSS) vulnerabilities in index.php in CubeCart 4.2.1 allow remote attackers to inject arbitrary web script or HTML via (1) the _a parameter in a searchStr action and the (2) Submit parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-31	4.3	CVE-2008-1550 SECUNIA
Digiappz -- digidomain	Multiple cross-site scripting (XSS) vulnerabilities in Digiappz DigiDomain 2.2 allow remote attackers to inject arbitrary web script or HTML via the (1) domain parameter to lookup_result.asp, and the (2) word1 and (3) word2 parameters to suggest_result.asp.	unknown 2008-03-31	4.3	CVE-2008-1560 BUGTRAQ BID SECUNIA XF
Easy Software Products -- CUPS	Integer overflow in pdftops filter in CUPS in Red Hat Enterprise Linux 3 and 4, when running on 64-bit platforms, allows remote attackers to execute arbitrary code via a crafted PDF file. NOTE: this issue is due to an incomplete fix for CVE-2004-0888.	unknown 2008-04-03	6.0	CVE-2008-1374 REDHAT
elastic_path -- elastic_path	Multiple directory traversal vulnerabilities in Elastic Path (EP) 4.1 and 4.1.1 allow remote attackers to (1) download arbitrary files via a .. (dot dot) in the file parameter to manager/getImportFileRedirect.jsp, (2) upload arbitrary files via a "..\" (dot dot backslash) in the file parameter to importData.jsp, and (3) list directory contents via a .. (dot dot) in the dir parameter to manager/fileManager.jsp.	unknown 2008-04-01	6.0	CVE-2008-1606 OTHER-REF OTHER-REF OTHER-REF BID SECUNIA XF XF

File-Transfer -- file_transfer	Directory traversal vulnerability in Dan Costin File Transfer before 1.2f allows remote attackers to read arbitrary files via a "..\" (dot dot backslash) in the filename.	unknown 2008-03-31	4.3	CVE-2008-1564 OTHER-REF OTHER-REF BID SECUNIA XF
Geertsen Holdings Inc -- GeeCarts	Multiple cross-site scripting (XSS) vulnerabilities in GeeCarts allow remote attackers to inject arbitrary web script or HTML via the id parameter to (1) show.php, (2) search.php, and (3) view.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-02	6.8	CVE-2008-1621 OTHER-REF BID XF
Geertsen Holdings Inc -- GeeCarts	Multiple PHP remote file inclusion vulnerabilities in GeeCarts allow remote attackers to execute arbitrary PHP code via a URL in the id parameter to (1) show.php, (2) search.php, and (3) view.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-02	6.8	CVE-2008-1622 BID XF
gnb -- designform	Cross-site scripting (XSS) vulnerability in GNB DesignForm before 3.9 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors in the email form.	unknown 2008-04-01	4.3	CVE-2008-1603 OTHER-REF OTHER-REF BID SECUNIA

IBM -- WebSphere MQ	MQSeries 5.1 in IBM WebSphere MQ 5.1 through 5.3.1 on the HP NonStop and Tandem NSK platforms does not require mqm group membership for execution of administrative tasks, which allows local users to bypass intended access restrictions via the runmqsc program, related to "Pathway panels."	unknown 2008-03-31	4.6	CVE-2008-1592 OTHER-REF FRSIRT SECTRACK
IBM -- AIX	The kernel in IBM AIX 5.2 and 5.3 does not properly handle resizing JFS2 filesystems on concurrent volume groups spread across multiple nodes, which allows local users of one node to cause a denial of service (remote node crash) by using chfs or lreducelv to reduce a filesystem's size.	unknown 2008-03-31	4.9	CVE-2008-1594 OTHER-REF OTHER-REF OTHER-REF AIXAPAR AIXAPAR AIXAPAR BID FRSIRT SECTRACK
IBM -- AIX	The proc filesystem in the kernel in IBM AIX 5.2 and 5.3 does not properly enforce directory permissions when a file executing from a directory has weaker permissions than the directory itself, which allows local users to obtain sensitive information.	unknown 2008-03-31	4.9	CVE-2008-1595 OTHER-REF OTHER-REF OTHER-REF AIXAPAR AIXAPAR AIXAPAR BID FRSIRT SECTRACK

IBM -- AIX	The WPAR system call implementation in the kernel in IBM AIX 6.1 allows local users to cause a denial of service via unknown calls that trigger "undefined behavior."	unknown 2008-03-31	4.9	CVE-2008-1597 OTHER-REF OTHER-REF OTHER-REF AIXAPAR AIXAPAR BID FRSIRT SECTRACK
IBM -- AIX	The kernel in IBM AIX 6.1 allows local users with ProbeVue privileges to read arbitrary kernel memory and obtain sensitive information via unspecified vectors.	unknown 2008-03-31	4.7	CVE-2008-1598 OTHER-REF OTHER-REF OTHER-REF AIXAPAR BID FRSIRT SECTRACK
jaf_cms -- jaf_cms	Multiple PHP remote file inclusion vulnerabilities in just another flat file (JAF) CMS 4.0 RC2 allow remote attackers to execute arbitrary PHP code via a URL in the (1) website parameter to (a) forum.php, (b) headlines.php, and (c) main.php in forum/, and (2) main_dir parameter to forum/forum.php. NOTE: other main_dir vectors are already covered by CVE-2006-7127.	unknown 2008-04-01	6.8	CVE-2008-1609 MILW0RM

Joomla -- Joomla	SQL injection vulnerability in the Bernard Gilly AlphaContent (com_alphacontent) 2.5.8 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a view action to index.php.	unknown 2008-03-31	6.8	CVE-2008-1559 MILW0RM BID XF
JV2 -- Folder Gallery	Cross-site scripting (XSS) vulnerability in index.php in JV2 Folder Gallery 3.1 allows remote attackers to inject arbitrary web script or HTML via the image parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-02	6.8	CVE-2008-1634 SECUNIA
JV2 -- Quick Gallery	Cross-site scripting (XSS) vulnerability in index.php in JV2 Quick Gallery 1.1 allows remote attackers to inject arbitrary web script or HTML via the f parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-02	6.8	CVE-2008-1636 SECUNIA
Linux -- Audit	Stack-based buffer overflow in the audit_log_user_command function in lib/audit_logging.c in Linux Audit before 1.7 might allow remote attackers to execute arbitrary code via a long command argument. NOTE: some of these details are obtained from third party information.	unknown 2008-04-02	4.1	CVE-2008-1628 OTHER-REF SECUNIA
ManageEngine -- Applications Manager	Cross-site scripting (XSS) vulnerability in Search.do in ManageEngine Applications Manager 8.x allows remote attackers to inject arbitrary web script or HTML via the query parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-31	4.3	CVE-2008-1566 BID SECUNIA
Mondo -- Rescue	Unspecified vulnerability in Mondo Rescue before 2.2.5 has unknown impact and attack vectors, related to the use of (1) /tmp and (2) MINDI_CACHE.	unknown 2008-04-02	4.6	CVE-2008-1633 OTHER-REF SECUNIA

MyioSoft -- EasyNews	Cross-site scripting (XSS) vulnerability in staticpages/easypublish/index.php in EasyNews 4.0 allows remote attackers to inject arbitrary web script or HTML via the read parameter in an edp_pupublish action.	unknown 2008-04-02	5.0	CVE-2008-1649 BUGTRAQ MILW0RM
NIK Software Inc -- NIK Sharpener Pro	Nik Sharpener Pro, possibly 2.0, uses world-writable permissions for plug-in files, which allows local users to gain privileges by replacing a plug-in with a Trojan horse.	unknown 2008-04-02	6.8	CVE-2008-1638 CERT-VN BID SECUNIA
Novell -- eDirectory	Stack-based buffer overflow in the DoLBURPRequest function in libnldap in ndsd in Novell eDirectory 8.7.3.9 and earlier, and 8.8.1 and earlier in the 8.8.x series, allows remote attackers to cause a denial of service (daemon crash or CPU consumption) and or arbitrary code via a long delRequest LDAP Extended Request message, probably involving a long Distinguished Name (DN) field.	unknown 2008-03-28	6.8	CVE-2008-0924 OTHER-REF FRSIRT SECUNIA BUGTRAQ OTHER-REF BID SECTRACK
OpenBSD -- Open_BSD OpenSSH -- OpenSSH	OpenSSH before 4.9 allows remote authenticated users to bypass the sshd_config ForceCommand directive by modifying the .ssh/rc session file.	unknown 2008-04-02	4.3	CVE-2008-1657 OTHER-REF OTHER-REF OPENBSD BID FRSIRT SECTRACK SECUNIA SECUNIA XF

Pau Rodriguez -- PHPkrm	Cross-site scripting (XSS) vulnerability in PHPkrm before 1.5.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-04-02	6.8	CVE-2008-1629 OTHER-REF SECUNIA
perlmailer -- perlmailer	Cross-site scripting (XSS) vulnerability in PerlMailer before 3.02 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-04-01	4.3	CVE-2008-1604 OTHER-REF OTHER-REF OTHER-REF BID SECUNIA
PierreEGougelet -- XnView	Stack-based buffer overflow in XnView 1.92 and 1.92.1 allows user-assisted remote attackers to execute arbitrary code via a long FontName parameter in a slideshow (.sld) file, a different vector than CVE-2008-1461.	unknown 2008-04-02	6.0	CVE-2008-0069 OTHER-REF FRSIRT SECUNIA
policyd-weight -- policyd-weight	policyd-weight before 0.1.14 beta-16 allows local users to modify or delete arbitrary files via a symlink attack on temporary files that are used when creating a socket.	unknown 2008-03-31	4.6	CVE-2008-1569 OTHER-REF OTHER-REF DEBIAN BID SECUNIA
policyd-weight -- policyd-weight	Race condition in the create_lockpath function in policyd-weight 0.1.14 beta-16 allows local users to modify or delete arbitrary files by creating the LOCKPATH directory, then modifying it after the symbolic link check occurs. NOTE: this is due to an incomplete fix for CVE-2008-1569.	unknown 2008-03-31	4.6	CVE-2008-1570 OTHER-REF

PowerDNS -- Recursor	PowerDNS Recursor before 3.1.5 uses insufficient randomness to calculate (1) TRXID values and (2) UDP source port numbers, which makes it easier for remote attackers to poison a DNS cache, related to (a) algorithmic deficiencies in rand and random functions in external libraries, (b) use of a 32-bit seed value, and (c) choice of the time of day as the sole seeding information.	unknown 2008-04-02	6.8	CVE-2008-1637 OTHER-REF OTHER-REF OTHER-REF FRSIRT SECUNIA
Red Hat -- lspp-eal4-config-ibm Red Hat -- capp-lspp-eal4-config-hp	The Replace function in the capp-lspp-config script in the (1) lspp-eal4-config-ibm and (2) capp-lspp-eal4-config-hp packages before 0.65-2 in Red Hat Enterprise Linux (RHEL) 5 uses lstat instead of stat to determine the /etc/pam.d/system-auth file permissions, leading to a change to world-writable permissions for the /etc/pam.d/system-auth-ac file, which allows local users to gain privileges by modifying this file.	unknown 2008-04-03	4.3	CVE-2008-0884 OTHER-REF REDHAT BID SECTRACK SECUNIA XF
Sebastian Marsching -- suPHP	suPHP before 0.6.3 allows local users to gain privileges via (1) a race condition that involves multiple symlink changes to point a file owned by a different user, or (2) a symlink to the directory of a different user, which is used to determine privileges.	unknown 2008-04-02	4.3	CVE-2008-1614 MLIST
Serby Arslanhan -- Bomba Haber	SQL injection vulnerability in haberoku.php in Serbay Arslanhan Bomba Haber 2.0 allows remote attackers to execute arbitrary SQL commands via the haber parameter.	unknown 2008-04-01	6.8	CVE-2008-1607 BID XF

SILC -- SILC Client SILC -- silc SILC -- silc_server SILC -- SILC Toolkit	The silc_pkcs1_decode function in the silccrypt library (silcpkcs1.c) in Secure Internet Live Conferencing (SILC) Toolkit before 1.1.7, SILC Client before 1.1.4, and SILC Server before 1.1.2 allows remote attackers to execute arbitrary code via a crafted PKCS#1 message, which triggers an integer underflow, signedness error, and a buffer overflow. NOTE: the researcher describes this as an integer overflow, but CVE uses the "underflow" term in cases of wraparound from unsigned subtraction.	unknown 2008-03-31	6.8	CVE-2008-1552 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECTRACK SECUNIA
Squid -- Squid	The arrayShrink function (lib/Array.c) in Squid 2.6.STABLE17 allows attackers to cause a denial of service (process exit) via unknown vectors that cause an array to shrink to 0 entries, which triggers an assert error. NOTE: this issue is due to an incorrect fix for CVE-2007-6239.	unknown 2008-04-01	4.3	CVE-2008-1612 OTHER-REF OTHER-REF MLIST MLIST
Topper -- TopperMod	Directory traversal vulnerability in mod.php in TopperMod 1.0 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the to parameter.	unknown 2008-03-31	4.6	CVE-2008-1553 MILW0RM BID
Topper -- TopperMod	SQL injection vulnerability in account/index.php in TopperMod 2.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via a non-alphanumeric first character the localita parameter, which bypasses a protection mechanism.	unknown 2008-03-31	6.8	CVE-2008-1554 MILW0RM BID

Wireshark -- Wireshark	The LDAP dissector in Wireshark (formerly Ethereal) 0.99.2 through 0.99.8 allows remote attackers to cause a denial of service (application crash) via a malformed packet, a different vulnerability than CVE-2006-5740.	unknown 2008-03-31	5.4	CVE-2008-1562 OTHER-REF BID FRSIRT SECUNIA
XenSource Inc -- Xen	The ssm_i emulation in Xen 5.1 on IA64 architectures allows attackers to cause a denial of service (dom0 panic) via certain traffic, as demonstrated using an FTP stress test tool.	unknown 2008-04-02	5.8	CVE-2008-1619 OTHER-REF

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered / Published	CVSS Score	Source & Patch Info
phpMyAdmin -- phpMyAdmin	phpMyAdmin before 2.11.5.1 stores the (1) MySQL username, (2) password, and the (2) Blowfish secret key in plaintext in the /tmp Session file, which allows local users to obtain sensitive information.	unknown 2008-03-31	2.1	CVE-2008-1567 OTHER-REF OTHER-REF FRSIRT SECUNIA
Wireshark -- Wireshark	Multiple unspecified vulnerabilities in Wireshark (formerly Ethereal) 0.99.5 through 0.99.8 allow remote attackers to cause a denial of service (application crash) via a malformed packet to the (1) X.509sat or (2) Roofnet dissectors. NOTE: Vector 2 might also lead to a hang.	unknown 2008-03-31	2.9	CVE-2008-1561 OTHER-REF BID FRSIRT SECUNIA

Wireshark -- Wireshark	The "decode as" feature in packet-bssap.c in the SCCP dissector in Wireshark (formerly Ethereal) 0.99.6 through 0.99.8 allows remote attackers to cause a denial of service (application crash) via a malformed packet.	unknown 2008-03-31	2.9	CVE-2008-1563 OTHER-REF BID FRSIRT SECUNIA

Back to top