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

Asterisk -- s800i Asterisk -- Asterisk Business Edition Asterisk -- Asterisk Appliance Developer Kit Asterisk -- AsteriskNOW Asterisk -- Open Source	Multiple buffer overflows in Asterisk Open Source 1.4.x before 1.4.18.1 and 1.4.19-rc3, Open Source 1.6.x before 1.6.0-beta6, Business Edition C.x.x before C.1.6.1, AsteriskNOW 1.0.x before 1.0.2, Appliance Developer Kit before 1.4 revision 109386, and s800i 1.1.x before 1.1.0.2 allow remote attackers to (1) write a zero to an arbitrary memory location via a large RTP payload number, related to the ast_rtp_unset_m_type function in main/rtp.c; or (2) write certain integers to an arbitrary memory location via a large number of RTP payloads, related to the process_sdp function in channels/chan_sip.c.	unknown 2008-03-24	7.5	CVE-2008-1289 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECTRACK SECUNIA
Asterisk -- s800i Asterisk -- Asterisk Appliance Developer Kit Asterisk -- AsteriskNOW Asterisk -- Asterisk Asterisk -- Asterisk Business Edition	The AsteriskGUI HTTP server in Asterisk Open Source 1.4.x before 1.4.19-rc3 and 1.6.x before 1.6.0-beta6, Business Edition C.x.x before C.1.6, AsteriskNOW before 1.0.2, Appliance Developer Kit before revision 104704, and s800i 1.0.x before 1.1.0.2 generates insufficiently random manager ID values, which makes it easier for remote attackers to hijack a manager session via a series of ID guesses.	unknown 2008-03-24	9.3	CVE-2008-1390 BUGTRAQ OTHER-REF BID SECUNIA
Asus -- Remote Console	Stack-based buffer overflow in the DPC Proxy server (DpcProxy.exe) in ASUS Remote Console (aka ARC or ASMB3) 2.0.0.19 and 2.0.0.24 allows remote attackers to execute arbitrary code via a long string to TCP port 623.	unknown 2008-03-25	10.0	CVE-2008-1491 BUGTRAQ OTHER-REF BID SECUNIA XF

Cisco -- Supervisor Engine Cisco -- Route Switch Processor	Unspecified vulnerability in the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720), and Route Switch Processor 720 (RSP720) for multiple Cisco products, when using Multi Protocol Label Switching (MPLS) VPN and OSPF sham-link, allows remote attackers to cause a denial of service (blocked queue, device restart, or memory leak) via unknown vectors.	unknown 2008-03-27	7.1	CVE-2008-0537 CISCO
Cisco -- Cisco IOS	The virtual private dial-up network (VPDN) component in Cisco IOS before 12.3 allows remote attackers to cause a denial of service (resource exhaustion) via a series of PPTP sessions, related to the persistence of interface descriptor block (IDB) data structures after process termination, aka bug ID CSCdv59309.	unknown 2008-03-27	7.1	CVE-2008-1150 CISCO BID SECTRACK
Cisco -- Cisco IOS	Memory leak in the virtual private dial-up network (VPDN) component in Cisco IOS before 12.3 allows remote attackers to cause a denial of service (memory consumption) via a series of PPTP sessions, related to "dead memory" that remains allocated after process termination, aka bug ID CSCsj58566.	unknown 2008-03-27	7.1	CVE-2008-1151 CISCO BID SECTRACK
Cisco -- Cisco IOS	The data-link switching (DLSw) component in Cisco IOS 12.0 through 12.4 allows remote attackers to cause a denial of service (device restart or memory consumption) via crafted (1) UDP port 2067 or (2) IP protocol 91 packets.	unknown 2008-03-27	7.8	CVE-2008-1152 CISCO BID
Cisco -- Cisco IOS	Cisco IOS 12.1, 12.2, 12.3, and 12.4 with IPv6 enabled allows remote attackers to cause a denial of service (device crash and possible blocked interface) via a crafted IPv6 packet to the device.	unknown 2008-03-27	7.1	CVE-2008-1153 CISCO

Computer Associates -- Unicenter DSM r11 List Control ATX Computer Associates -- BrightStor ARCserve Backup Laptops_Desktops	Stack-based buffer overflow in the ListCtrl.ocx ActiveX Control in CA BrightStor ARCserve Backup R11.5 allows remote attackers to execute arbitrary code or cause a denial of service (crash) via a long argument to the AddColumn method.	unknown 2008-03-24	9.3	CVE-2008-1472 MILW0RM BID FRSIRT SECUNIA XF
CoronaMatrix -- phpAddressBook	Multiple directory traversal vulnerabilities in CoronaMatrix phpAddressBook 2.11 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the skin parameter to (1) index.php and (2) install.php.	unknown 2008-03-25	7.5	CVE-2008-1492 BUGTRAQ MILW0RM OTHER-REF BID
Cuteflow -- Bin	Directory traversal vulnerability in login.php in Cuteflow Bin 1.5.0 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the language parameter.	unknown 2008-03-25	7.5	CVE-2008-1493 MILW0RM
Detodas -- Restaurante component for Joomla	SQL injection vulnerability in the Detodas Restaurante (com_restaurante) 1.0 component for Mambo and Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a detail action to index.php, a different product than CVE-2008-0562.	unknown 2008-03-24	9.3	CVE-2008-1465 MILW0RM BID SECUNIA XF
Easy-Clanpage -- Easy-Clanpage	SQL injection vulnerability in inc/module/online.php in Easy-Clanpage 2.2 allows remote attackers to execute arbitrary SQL commands via the id parameter in a user details action, a different vector than CVE-2008-1425.	unknown 2008-03-25	7.5	CVE-2008-1494 BUGTRAQ BID
EfesTech -- Kontor	SQL injection vulnerability in EfesTech E-Kontör and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-03-25	7.5	CVE-2008-1508 BUGTRAQ BID

FreeBSD -- FreeBSD NetBSD -- NetBSD	Multiple integer overflows in libc in NetBSD 4.x, FreeBSD 6.x and 7.x, and probably other BSD and Apple Mac OS platforms allow context-dependent attackers to execute arbitrary code via large values of certain integer fields in the format argument to (1) the strfmon function in lib/libc/stdlib/strfmon.c, related to the GET_NUMBER macro; and (2) the printf function, related to left_prec and right_prec.	unknown 2008-03-27	7.5	CVE-2008-1391 SREASONRES SREASON
FreeWebShop -- FreeWebShop	Unspecified vulnerability in customer.php in FreeWebshop.org 2.2.5, 2.2.6 and 2.2.7WIP1/2 allows remote attackers to gain administrator privileges via unknown vectors.	unknown 2008-03-24	10.0	CVE-2007-6711 OTHER-REF OTHER-REF
Gallarific -- Gallarific	Multiple SQL injection vulnerabilities in Gallarific Free Edition 1.1 allow remote attackers to execute arbitrary SQL commands via the (1) query parameter to (a) search.php; (2) gusername and (3) gpassword parameters to (b) login.php; and the (4) username and (5) password parameters to (c) gadmin/index.php in a signin action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-24	7.5	CVE-2008-1464 SECUNIA
GnuPG -- GnuPG	GnuPG (gpg) 1.4.8 and 2.0.8 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted duplicate keys that are imported from key servers, which triggers "memory corruption around deduplication of user IDs."	unknown 2008-03-27	7.5	CVE-2008-1530 OTHER-REF OTHER-REF OTHER-REF

Joomla -- com_alberghi Mambo -- com_alberghi	SQL injection vulnerability in the Alberghi (com_alberghi) 2.1.3 and earlier component for Mambo and Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a detail action to index.php.	unknown 2008-03-24	7.5	CVE-2008-1459 MILW0RM BID SECUNIA XF
Joomla -- com_custompages SSTREAMTV -- Custompages	PHP remote file inclusion vulnerability in the SSTREAMTV custompages (com_custompages) 1.1 and earlier component for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the cpage parameter to index.php.	unknown 2008-03-25	7.5	CVE-2008-1505 MILW0RM BID
Mambo -- com_joovideo Joomla -- com_joovideo Joomlapixel -- Joovideo	SQL injection vulnerability in the Joovideo (com_joovideo) 1.0 and 1.2.2 component for Mambo and Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a detail action to index.php.	unknown 2008-03-24	7.5	CVE-2008-1460 MILW0RM BID SECUNIA XF
Microsoft -- windows-nt	Microsoft Windows Vista does not properly enforce the NoDriveTypeAutoRun registry value, which allows user-assisted remote attackers, and possibly physically proximate attackers, to execute arbitrary code by inserting a (1) CD-ROM device or (2) U3-enabled USB device containing a filesystem with an Autorun.inf file, and possibly other vectors related to (a) AutoRun and (b) AutoPlay actions.	unknown 2008-03-24	9.3	CVE-2008-0951 CERT-VN BID
Microsoft -- Word	Buffer overflow in msjet40.dll before 4.0.9505.0 in Microsoft Jet Database Engine allows remote attackers to execute arbitrary code via a crafted Word file, as exploited in the wild in March 2008. NOTE: this issue might be related to CVE-2007-6026.	unknown 2008-03-25	9.3	CVE-2008-1092 MSKB CERT-VN SECTRACK XF

Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Unspecified vulnerability in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allows remote attackers to execute arbitrary code via "XPCNativeWrapper pollution."	unknown 2008-03-27	7.5	CVE-2008-1233 OTHER-REF
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Unspecified vulnerability in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allows remote attackers to execute arbitrary code via unknown vectors that cause JavaaScript to execute with the wrong principal, aka "Privilege escalation via incorrect principals."	unknown 2008-03-27	7.5	CVE-2008-1235 OTHER-REF
NetWin -- SurgeMail	Stack-based buffer overflow in the IMAP service in NetWin Surgemail 3.8k4-4 and earlier allows remote authenticated users to execute arbitrary code via a long first argument to the LIST command.	unknown 2008-03-25	9.0	CVE-2008-1498 MILW0RM OTHER-REF FRSIRT SECUNIA
Novell -- eDirectory	Unspecified vulnerability in the eMBox utility in Novell eDirectory 8.7.3.9 and earlier, and 8.8.x before 8.8.2, allows remote attackers to cause a denial of service or access local files via unknown vectors, probably involving unauthenticated SOAP requests.	unknown 2008-03-28	7.5	CVE-2008-0926 OTHER-REF FRSIRT SECUNIA
Panda -- Panda Internet Security Panda -- Panda Antivirus and Firewall	The cpoint.sys driver in Panda Internet Security 2008 and Antivirus+ Firewall 2008 allows local users to cause a denial of service (system crash or kernel panic), overwrite memory, or execute arbitrary code via a crafted IOCTL request that triggers an out-of-bounds write of kernel memory.	unknown 2008-03-24	7.2	CVE-2008-1471 OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECTRACK SECUNIA XF

Peel -- Peel	Multiple SQL injection vulnerabilities in PEEL, possibly 3.x and earlier, allow remote attackers to execute arbitrary SQL commands via the (1) email parameter to (a) membre.php, and the (2) timestamp parameter to (b) the details action in achat/historique_commandes.php and (c) the facture action in factures/facture_html.php.	unknown 2008-03-25	7.5	CVE-2008-1496 MILW0RM OTHER-REF BID SECUNIA XF XF
Peel -- Peel	PEEL, possibly 3.x and earlier, has (1) a default info@peel.fr account with password admin, and (2) a default contact@peel.fr account with password cinema, which allows remote attackers to gain administrative access.	unknown 2008-03-25	7.5	CVE-2008-1507 MILW0RM OTHER-REF
phpBB -- Module XS	Directory traversal vulnerability in admin/admin_xs.php in phpBB Module XS 2.3.1 allows remote attackers to include and execute arbitrary files via a .. (dot dot) in the phpEx parameter.	unknown 2008-03-25	7.5	CVE-2008-1512 MILW0RM
Piczo -- ImageUploader4 Aurigma -- Image Uploader ActiveX control	Buffer overflow in a certain Aurigma ActiveX control in ImageUploader4.ocx 4.1.36.0, as used with Piczo (aka Pizco) and possibly other online services, allows remote attackers to execute arbitrary code via unspecified vectors, possibly involving a long Action property, a different CLSID than CVE-2008-0659.	unknown 2008-03-25	9.3	CVE-2008-1490 BUGTRAQ BID SECUNIA XF
PowerScripts -- PowerPHPBoard	Multiple directory traversal vulnerabilities in PowerPHPBoard 1.00b allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) settings[footer] parameter to footer.inc.php and the (2) settings[header] parameter to header.inc.php.	unknown 2008-03-28	7.5	CVE-2008-1534 BUGTRAQ MILW0RM

Symantec -- Altiris Deployment Solution	The Altiris Client Service (AClient.exe) in Symantec Altiris Deployment Solution 6.8.x to 6.9.164 allows local users to gain privileges via a "Shatter" style attack.	unknown 2008-03-24	7.2	CVE-2008-1473 OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
XLPortal -- XLPortal	SQL injection vulnerability in index.php in XLPortal 2.2.4 and earlier allows remote attackers to execute arbitrary SQL commands via the query parameter.	unknown 2008-03-25	7.5	CVE-2008-1509 MILW0RM BID
XnView -- XnView Standard	Buffer overflow in XnView 1.92.1 allows user-assisted remote attackers to execute arbitrary code via a long filename argument on the command line. NOTE: it is unclear whether there are common handler configurations in which this argument is controlled by an attacker.	unknown 2008-03-24	7.6	CVE-2008-1461 BUGTRAQ OTHER-REF BID XF
ZyXEL -- ZyWALL	ZyXEL ZyWALL 1050 has a hard-coded password for the Quagga and Zebra processes that is not changed when it is set by a user, which allows remote attackers to gain privileges.	unknown 2008-03-24	7.5	CVE-2008-1160 OTHER-REF OTHER-REF MILW0RM BID
ZyXEL -- Prestige 661 ZyXEL -- Prestige 660 ZyXEL -- ZyNOS	ZyXEL Prestige routers, including P-660 and P-661 models with firmware 3.40 (AGD.2) through 3.40(AHQ.3), have (1) "user" as their default password for the "user" account and (2) "1234" as their default password for the "admin" account, which makes it easier for remote attackers to obtain access.	unknown 2008-03-26	7.5	CVE-2008-1522 BUGTRAQ OTHER-REF OTHER-REF

ZyXEL -- Prestige 661 ZyXEL -- Prestige 660 ZyXEL -- ZyNOS	The SNMP service on ZyXEL Prestige routers, including P-660 and P-661 models with firmware 3.40(AGD.2) through 3.40(AHQ.3), has "public" as its default community for both (1) read and (2) write operations, which allows remote attackers to perform administrative actions via SNMP, as demonstrated by reading the Dynamic DNS service password or inserting an XSS sequence into the system. sysName.0 variable, which is displayed on the System Status page.	unknown 2008-03-26	7.5	CVE-2008-1524 BUGTRAQ OTHER-REF OTHER-REF
ZyXEL -- Prestige 661 ZyXEL -- Prestige 660 ZyXEL -- ZyNOS	ZyXEL Prestige routers, including P-660, P-661, and P-662 models with firmware 3.40(PE9) and 3.40(AGD.2) through 3.40(AHQ.3), support authentication over HTTP via a hash string in the hiddenPassword field, which allows remote attackers to obtain access via a replay attack.	unknown 2008-03-26	7.5	CVE-2008-1527 BUGTRAQ OTHER-REF OTHER-REF

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Alkacon -- OpenCms	Cross-site scripting (XSS) vulnerability in system/workplace/admin/accounts/users_list.jsp in Alkacon OpenCMS 7.0.3 allows remote attackers to inject arbitrary web script or HTML via the (1) searchfilter or (2) listSearchFilter parameter.	unknown 2008-03-25	4.3	CVE-2008-1510 BUGTRAQ BID XF

CenterIM -- CenterIM	CenterIM 4.22.3 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in a URI, related to "received URLs in the message window."	unknown 2008-03-24	6.8	CVE-2008-1467 MILW0RM BID FRSIRT SECUNIA
Cisco -- Cisco IOS	Unspecified vulnerability in the Multicast Virtual Private Network (MVPN) implementation in Cisco IOS 12.0, 12.2, 12.3, and 12.4 allows remote attackers to create "extra multicast states on the core routers" via a crafted Multicast Distribution Tree (MDT) Data Join message.	unknown 2008-03-27	5.1	CVE-2008-1156 CISCO
cPanel -- cPanel	Cross-site scripting (XSS) vulnerability in frontend/x/manpage.html in cPanel 11.18.3 and 11.21.0-BETA allows remote attackers to inject arbitrary web script or HTML via the query string.	unknown 2008-03-25	4.3	CVE-2008-1499 BUGTRAQ BID XF
CS-Cart -- CS-Cart	Cross-site scripting (XSS) vulnerability in index.php in CS-Cart 1.3.2 allows remote attackers to inject arbitrary web script or HTML via the q parameter in a products search action.	unknown 2008-03-24	4.3	CVE-2008-1458 BUGTRAQ BID
cyberfrogs -- cfnetgs	Cross-site scripting (XSS) vulnerability in index.php in cyberfrogs.net cfnetgs 0.24 allows remote attackers to inject arbitrary web script or HTML via the directory parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-24	4.3	CVE-2008-1479 BID XF
Danneo -- CMS	SQL injection vulnerability in index.php in Danneo CMS 0.5.1 and earlier, when the Referers statistics option is enabled, allows remote attackers to execute arbitrary SQL commands via the HTTP Referer header.	unknown 2008-03-25	6.8	CVE-2008-1513 MILW0RM XF

eGroupWare -- eGroupWare	The _bad_protocol_once function in phpgwapi/inc/class.kses.inc.php in eGroupWare before 1.4.003 allows remote attackers to bypass HTML filtering and conduct cross-site scripting (XSS) attacks via a string containing crafted URL protocols.	unknown 2008-03-25	4.3	CVE-2008-1502 OTHER-REF OTHER-REF SECUNIA
F5 -- BIG-IP	Cross-site scripting (XSS) vulnerability in the web management interface in F5 BIG-IP 9.4.3 allows remote attackers to inject arbitrary web script or HTML via (1) the name of a node object, or the (2) sysContact or (3) sysLocation SNMP configuration field, aka "Audit Log XSS." NOTE: these issues might be resultant from cross-site request forgery (CSRF) vulnerabilities.	unknown 2008-03-25	4.3	CVE-2008-1503 BUGTRAQ BID
fedoraproject -- fedora Linux -- Kernel	ptrace in Linux kernel 2.6.9 on Fedora 7 and 8 allows local users to cause a denial of service (kernel panic) via the user-area-padding test from the ptrace testsuite, which triggers an invalid dereference.	unknown 2008-03-25	4.9	CVE-2008-1514 OTHER-REF OTHER-REF
FutureNuke -- PHP_Nuke Platinum	SQL injection vulnerability in includes/dynamic_titles.php in PHP-Nuke Platinum 7.6.b.5 allows remote attackers to execute arbitrary SQL commands via the p parameter to modules.php for the Forums module.	unknown 2008-03-28	6.8	CVE-2008-1539 MILW0RM BID XF
Gallarific -- Gallarific	Gallarific Free Edition 1.1 does not require authentication for (1) photos.php, (2) comments.php, and (3) gallery.php in gadmin/, which allows remote attackers to edit objects via a direct request, different vectors than CVE-2008-1327. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-24	5.0	CVE-2008-1469 SECUNIA

HIS -- Webshop	Directory traversal vulnerability in cgi-bin/his-webshop.pl in HIS Webshop 2.50 allows remote attackers to read arbitrary files via a .. (dot dot) in the t parameter.	unknown 2008-03-28	5.8	CVE-2008-1541 BUGTRAQ MILW0RM BID FRSIRT XF
Home Ftp Server -- Home Ftp Server	Home FTP Server 1.4.5.89 allows remote attackers to cause a denial of service (crash) by opening a FTP passive mode connection, then closing the original FTP connection. NOTE: some of these details are obtained from third party information.	unknown 2008-03-24	5.0	CVE-2008-1478 BUGTRAQ BID SECUNIA
Imperva -- SecureSphere MX Management Server Imperva -- SecureSphere	Cross-site scripting (XSS) vulnerability in the management GUI in Imperva SecureSphere MX Management Server 5.0 allows remote attackers to inject arbitrary web script or HTML via an invalid or prohibited request to a web server protected by SecureSphere, which triggers injection into the "corrective action" section of an alert page.	unknown 2008-03-24	4.3	CVE-2008-1463 OTHER-REF BID SECUNIA
IRCU -- IRCU QuakeNet -- snircd	The send_user_mode function in s_user.c in (1) Undernet ircu 2.10.12.12 and earlier, (2) snircd 1.3.4 and earlier, and unspecified other ircu derivatives allows remote attackers to cause a denial of service (daemon crash) via a malformed MODE command.	unknown 2008-03-25	5.0	CVE-2008-1501 BUGTRAQ FULLDISC OTHER-REF SECUNIA SECUNIA
JCorporate -- eForum	Multiple cross-site scripting (XSS) vulnerabilities in busca.php in eForum 0.4 allow remote attackers to inject arbitrary web script or HTML via the (1) busca and (2) link parameters.	unknown 2008-03-24	4.3	CVE-2008-1477 BUGTRAQ OTHER-REF SECUNIA

Joomla -- Joomla	Unspecified vulnerability in the XML-RPC Blogger API plugin in Joomla! 1.5 allows remote attackers to perform unauthorized article operations on articles via unknown vectors.	unknown 2008-03-27	6.8	CVE-2008-1533 OTHER-REF SECUNIA
Joomla -- Datsogallery Mambo -- Datsogallery	SQL injection vulnerability in the Datsogallery (com_datsogallery) 1.3.1 module for Joomla! and Mambo allows remote attackers to execute arbitrary SQL commands via the id parameter in a detail action to index.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-28	6.8	CVE-2008-1540 BID XF
lighttpd -- lighttpd	lighttpd 1.4.19 and earlier allows remote attackers to cause a denial of service (active SSL connection loss) by triggering an SSL error, such as disconnecting before a download has finished, which causes all active SSL connections to be lost.	unknown 2008-03-27	4.3	CVE-2008-1531 OTHER-REF OTHER-REF OTHER-REF
LinPHA -- LinPHA	Multiple cross-site scripting (XSS) vulnerabilities in LinPHA before 1.3.3 allow remote attackers to inject arbitrary web script or HTML via (1) ftp/index.php, (2) viewer.php, (3) functions/other.php, (4) include/left_menu.class.php, and (5) plugins/stats/stats_view.php.	unknown 2008-03-24	4.3	CVE-2008-1487 OTHER-REF OTHER-REF
ManageEngine -- EventLog Analyzer	Cross-site scripting (XSS) vulnerability in searchAction.do in ManageEngine EventLog Analyzer 5 allows remote attackers to inject arbitrary web script or HTML via the searchText parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-28	6.8	CVE-2008-1538 SECUNIA

Matti Kiviharju -- Rekry Component	SQL injection vulnerability in the Matti Kiviharju rekry (aka com_rekry or rekry! Joom) 1.0.0 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the op_id parameter in a view action to index.php.	unknown 2008-03-28	6.4	CVE-2008-1535 MILW0RM BID SECUNIA XF
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allows remote attackers to inject arbitrary web script or HTML via event handlers, aka "Universal XSS using event handlers."	unknown 2008-03-27	4.3	CVE-2008-1234 OTHER-REF
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors related to the layout engine.	unknown 2008-03-27	6.8	CVE-2008-1236 OTHER-REF
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors related to the JavaScript engine.	unknown 2008-03-27	6.8	CVE-2008-1237 OTHER-REF
Mozilla -- SeaMonkey Mozilla -- Firefox	Mozilla Firefox before 2.0.0.13 and SeaMonkey before 1.1.9, when generating the HTTP Referer header, does not list the entire URL when it contains Basic Authentication credentials without a username, which makes it easier for remote attackers to bypass application protection mechanisms that rely on Referer headers, such as with some Cross-Site Request Forgery (CSRF) mechanisms.	unknown 2008-03-27	5.0	CVE-2008-1238 OTHER-REF OTHER-REF

Mozilla -- SeaMonkey Mozilla -- Firefox	LiveConnect in Mozilla Firefox before 2.0.0.13 and SeaMonkey before 1.1.9 does not properly parse the content origin for jar: URIs before sending them to the Java plugin, which allows remote attackers to access arbitrary ports on the local machine. NOTE: this is closely related to CVE-2008-1195.	unknown 2008-03-27	5.0	CVE-2008-1240 OTHER-REF
Mozilla -- SeaMonkey Mozilla -- Firefox	GUI overlay vulnerability in Mozilla Firefox before 2.0.0.13 and SeaMonkey before 1.1.9 allows remote attackers to spoof form elements and redirect user inputs via a borderless XUL pop-up window from a background tab.	unknown 2008-03-27	4.3	CVE-2008-1241 OTHER-REF
Namazu -- Namazu	Cross-site scripting (XSS) vulnerability in namazu.cgi in Namazu before 2.0.18 allows remote attackers to inject arbitrary web script or HTML via UTF-7 encoded input, related to failure to set the charset, a different vector than CVE-2004-1318 and CVE-2001-1350. NOTE: some of these details are obtained from third party information.	unknown 2008-03-24	4.3	CVE-2008-1468 OTHER-REF OTHER-REF SECUNIA
Novell -- eDirectory	Stack-based buffer overflow in the DoLBURPRequest function 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 possibly execute arbitrary code via a long 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

ooComments -- ooComments	Multiple PHP remote file inclusion vulnerabilities in ooComments 1.0 allow remote attackers to execute arbitrary PHP code via a URL in the PathToComment parameter for (1) classes/class_admin.php and (2) classes/class_comments.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-25	6.8	CVE-2008-1511 OTHER-REF BID
OpenSSH -- OpenSSH	OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.	unknown 2008-03-24	6.0	CVE-2008-1483 OTHER-REF
PECL-PHP -- Alternative PHP Cache	Stack-based buffer overflow in apc.c in Alternative PHP Cache (APC) 3.0.11 through 3.0.16 allows remote attackers to execute arbitrary code via a long filename.	unknown 2008-03-24	6.8	CVE-2008-1488 OTHER-REF OTHER-REF
Peel -- Peel	Unrestricted file upload vulnerability in administrer/produits.php in PEEL, possibly 3.x and earlier, allows remote authenticated administrators to upload and execute arbitrary PHP files via a modified content type in an ajout action, as demonstrated by (1) image/gif and (2) application/pdf.	unknown 2008-03-25	6.5	CVE-2008-1495 MILW0RM OTHER-REF BID SECUNIA XF
Peel -- Peel	PEEL, possibly 3.x and earlier, allows remote attackers to obtain configuration information via a direct request to phpinfo.php, which calls the phpinfo function.	unknown 2008-03-25	5.0	CVE-2008-1506 MILW0RM OTHER-REF

perlbal -- perlbal	Perlbal before 1.70, when buffered upload is enabled, allows remote attackers to cause a denial of service (crash) via a zero-byte chunked upload.	unknown 2008-03-27	5.0	CVE-2008-1532 OTHER-REF OTHER-REF OTHER-REF
Phorum -- Phorum	SQL injection vulnerability in Phorum before 5.2.6 , when mysql_use_ft is disabled, allows remote attackers to execute arbitrary SQL commands via the non-fulltext search.	unknown 2008-03-24	6.8	CVE-2008-1486 OTHER-REF
PHP -- PHP	Integer overflow in PHP 5.2.5 and earlier allows context-dependent attackers to cause a denial of service and possibly have unspecified other impact via a printf format parameter with a large width specifier, related to the php_sprintf_appendstring function in formatted_print.c and probably other functions for formatted strings (aka *printf functions).	unknown 2008-03-27	5.0	CVE-2008-1384 SREASONRES BUGTRAQ OTHER-REF BID
phpHeaven -- phpMyChat	Cross-site scripting (XSS) vulnerability in setup.php3 in phpHeaven phpMyChat 0.14.5 allows remote attackers to inject arbitrary web script or HTML via the Lang parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-25	4.3	CVE-2008-1504 BID XF
PHPStats -- phpstats	Cross-site scripting (XSS) vulnerability in phpstats.php in Michael Wagner phpstats 0.1 alpha allows remote attackers to inject arbitrary web script or HTML via the baseDir parameter.	unknown 2008-03-24	4.3	CVE-2008-0125 BUGTRAQ BID
PicturesPro -- PicturesPro Photo Cart	Cross-site scripting (XSS) vulnerability in index.php in Pictures Pro (aka Tim Grissett) Photo Cart 4.1 allows remote attackers to inject arbitrary web script or HTML via the amessage parameter. NOTE: some of these details are obtained from third party information.	unknown 2008-03-28	6.8	CVE-2008-1536 OTHER-REF BID SECUNIA

PowerScripts -- PowerBook	Directory traversal vulnerability in pb_inc/admincenter/index.php in PowerScripts PowerBook 1.21 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page parameter. NOTE: in some environments, this can be leveraged for remote file inclusion by using a UNC share pathname or an ftp, ftps, or ssh2. sftp URL.	unknown 2008-03-28	6.8	CVE-2008-1537 BUGTRAQ MILW0RM BID XF
PunBB -- PunBB	Cross-site scripting (XSS) vulnerability in PunBB 1.2.16 and earlier allows remote attackers to inject arbitrary web script or HTML via the get_host parameter to moderate.php.	unknown 2008-03-24	4.3	CVE-2008-1485 OTHER-REF SECUNIA
Roundup -- Roundup	Multiple unspecified vulnerabilities in Roundup before 1.4.4 have unknown impact and attack vectors.	unknown 2008-03-24	5.0	CVE-2008-1474 OTHER-REF OTHER-REF FEDORA FEDORA BID FRSIRT SECUNIA SECUNIA XF
Roundup -- Roundup	The xml-rpc server in Roundup 1.4.4 does not check property permissions, which allows attackers to bypass restrictions and edit or read restricted properties via the (1) list, (2) display, and (3) set methods.	unknown 2008-03-24	6.4	CVE-2008-1475 OTHER-REF OTHER-REF FEDORA FEDORA BID FRSIRT SECUNIA SECUNIA XF

RSA -- WebID	Incomplete blacklist vulnerability in IISWebAgentIF.dll in the WebID RSA Authentication Agent 5.3, and possibly earlier, allows remote attackers to conduct cross-site scripting (XSS) attacks via the postdata parameter, due to an incomplete fix for CVE-2005-1118.	unknown 2008-03-24	4.3	CVE-2008-1470 BUGTRAQ BID
RunCMS -- RunCMS	SQL injection vulnerability in the sections (Section) module in RunCMS allows remote attackers to execute arbitrary SQL commands via the artid parameter in a viewarticle action.	unknown 2008-03-24	6.8	CVE-2008-1462 MILW0RM BID
Serendipity -- Serendipity	Cross-site scripting (XSS) vulnerability in Serendipity (S9Y) before 1.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to received trackbacks.	unknown 2008-03-24	4.3	CVE-2008-1476 OTHER-REF SECUNIA
Sun -- Solaris	rpc.metad in Sun Solaris 10 allows remote attackers to cause a denial of service (daemon crash) via a malformed RPC request.	unknown 2008-03-24	4.3	CVE-2008-1480 MILW0RM BID FRSIRT SECUNIA XF
Tiny Portal -- Tiny Portal	Cross-site scripting (XSS) vulnerability in index.php in TinyPortal 0.8.6 and 1.0.3 allows remote attackers to inject arbitrary web script or HTML via the PHPSESSID parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-25	4.3	CVE-2008-1500 BID XF

VideoLAN -- VLC	Integer overflow in the MP4_ReadBox_rdrf function in libmp4.c for VLC 0.8.6e allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted MP4 RDRF box that triggers a heap-based buffer overflow, a different vulnerability than CVE-2008-0984.	unknown 2008-03-24	6.8	CVE-2008-1489 OTHER-REF
ViewVC -- ViewVC	ViewVC before 1.0.5 includes "all-forbidden" files within search results that list CVS or Subversion (SVN) commits, which allows remote attackers to obtain sensitive information.	unknown 2008-03-24	4.3	CVE-2008-1290 OTHER-REF OTHER-REF OTHER-REF GENTOO BID SECUNIA SECUNIA
ViewVC -- ViewVC	ViewVC before 1.0.5 stores sensitive information under the web root with insufficient access control, which allows remote attackers to read files and list folders under the hidden CVSROOT folder.	unknown 2008-03-24	4.3	CVE-2008-1291 OTHER-REF OTHER-REF OTHER-REF GENTOO BID SECUNIA SECUNIA
ViewVC -- ViewVC	ViewVC before 1.0.5 provides revision metadata without properly checking whether access was intended, which allows remote attackers to obtain sensitive information by reading (1) forbidden pathnames in the revision view, (2) log history that can only be reached by traversing a forbidden object, or (3) forbidden diff view path parameters.	unknown 2008-03-24	4.3	CVE-2008-1292 OTHER-REF OTHER-REF OTHER-REF GENTOO BID SECUNIA SECUNIA

W-Agora -- W-Agora	Multiple PHP remote file inclusion vulnerabilities in W-Agora 4.0 allow remote attackers to execute arbitrary PHP code via a URL in the bn_dir_default parameter to (1) add_user.php, (2) create_forum.php, (3) create_user.php, (4) delete_notes.php, (5) delete_user.php, (6) edit_forum.php, (7) mail_users.php, (8) moderate_notes.php, and (9) reorder_forums.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-24	6.8	CVE-2008-1466 BID
webSPELL -- webSPELL	Cross-site scripting (XSS) vulnerability in index.php in webSPELL 4.1.2 allows remote attackers to inject arbitrary web script or HTML via the board parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-24	4.3	CVE-2008-1481 OTHER-REF BID
xine -- xine-lib	Array index error in the sdpplin_parse function in input/libreal/sdpplin.c in xine-lib 1.1.10.1 allows remote RTSP servers to execute arbitrary code via a large streamid SDP parameter.	unknown 2008-03-24	6.8	CVE-2008-0073 OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECUNIA
xine -- xine-lib	Multiple integer overflows in xine-lib 1.1.11 and earlier allow remote attackers to trigger heap-based buffer overflows and possibly execute arbitrary code via (1) a crafted .FLV file, which triggers an overflow in demuxers/demux_flv.c; (2) a crafted .MOV file, which triggers an overflow in demuxers/demux_qt.c; (3) a crafted .RM file, which triggers an overflow in demuxers/demux_real.c; (4) a crafted .MVE file, which triggers an	unknown 2008-03-24	6.8	CVE-2008-1482 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF

	overflow in demuxers/demux_wc3movie.c; (5) a crafted .MKV file, which triggers an overflow in demuxers/ebml.c; or (6) a crafted .CAK file, which triggers an overflow in demuxers/demux_film.c.			BID
ZyXEL -- Prestige 661 ZyXEL -- Prestige 660 ZyXEL -- ZyNOS	ZyXEL Prestige routers, including P-660 and P-661 models with firmware 3.40 (AGD.2) through 3.40(AHQ.3), allow remote authenticated users to gain privileges by accessing administrative URIs, as demonstrated by rpSysAdmin.html.	unknown 2008-03-26	6.5	CVE-2008-1521 BUGTRAQ OTHER-REF OTHER-REF
ZyXEL -- Prestige 661 ZyXEL -- Prestige 660 ZyXEL -- ZyNOS	ZyXEL Prestige routers, including P-660, P-661, and P-662 models with firmware 3.40(AGD.2) through 3.40(AHQ.3), allow remote authenticated users to obtain ISP and Dynamic DNS credentials by sending a direct request for (1) WAN.html, (2) wzPPPOE.html, and (3) rpDyDNS.html, and then reading the HTML source.	unknown 2008-03-26	5.0	CVE-2008-1523 BUGTRAQ OTHER-REF OTHER-REF
ZyXEL -- Prestige 661 ZyXEL -- Prestige 660 ZyXEL -- ZyNOS	The default SNMP configuration on ZyXEL Prestige routers, including P-660 and P-661 models with firmware 3.40 (AGD.2) through 3.40(AHQ.3), has a Trusted Host value of 0.0.0.0, which allows remote attackers to send SNMP requests from any source IP address.	unknown 2008-03-26	5.0	CVE-2008-1525 BUGTRAQ OTHER-REF OTHER-REF
ZyXEL -- Prestige 661 ZyXEL -- Prestige 660 ZyXEL -- ZyNOS	ZyXEL Prestige routers, including P-660, P-661, and P-662 models with firmware 3.40(PE9) and 3.40(AGD.2) through 3.40 (AHQ.3), do not use a salt when calculating an MD5 password hash, which makes it easier for attackers to crack passwords.	unknown 2008-03-26	5.0	CVE-2008-1526 BUGTRAQ OTHER-REF OTHER-REF

ZyXEL -- Prestige 661 ZyXEL -- Prestige 660 ZyXEL -- ZyNOS	ZyXEL Prestige routers, including P-660, P-661, and P-662 models with firmware 3.40(AGD.2) through 3.40(AHQ.3), allow remote authenticated users to obtain authentication data by making direct HTTP requests and then reading the HTML source, as demonstrated by a request for (1) RemMagSNMP.html, which discloses SNMP communities; or (2) WLAN.html, which discloses WEP keys.	unknown 2008-03-26	4.0	CVE-2008-1528 BUGTRAQ OTHER-REF OTHER-REF
ZyXEL -- Prestige 661 ZyXEL -- Prestige 660 ZyXEL -- ZyNOS	ZyXEL Prestige routers have a minimum password length for the admin account that is too small, which makes it easier for remote attackers to guess passwords via brute force methods.	unknown 2008-03-26	5.0	CVE-2008-1529 BUGTRAQ OTHER-REF OTHER-REF

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered / Published	CVSS Score	Source & Patch Info
NetWin -- SurgeMail	Stack-based buffer overflow in the IMAP service in NetWin SurgeMail 38k4-4 and earlier allows remote authenticated users to execute arbitrary code via long arguments to the LSUB command.	unknown 2008-03-25	0.0	CVE-2008-1497 BUGTRAQ OTHER-REF OTHER-REF BID SECUNIA

PunBB -- PunBB	The password reset feature in PunBB 1.2.16 and earlier uses predictable random numbers based on the system time, which allows remote authenticated users to determine the new password via a brute force attack on a seed that is based on the approximate creation time of the targeted account. NOTE: this issue might be related to CVE-2006-5737.	unknown 2008-03-24	3.5	CVE-2008-1484 OTHER-REF MILW0RM OTHER-REF OTHER-REF BID SECUNIA

Back to top