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 | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| adobe -- flash_player | Multiple unspecified vulnerabilities in Adobe Flash Player 10.x before 10.0.12.36 and 9.x before 9.0.151.0 allow remote attackers to execute arbitrary code via unknown vectors related to "input validation errors." | 2008-11-17 | 9.3 | CVE-2008-4824<br>CONFIRM |
| apple -- safari | Heap-based buffer overflow in CoreGraphics in Apple Safari before 3.2 on Windows allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted image, related to improper handling of color spaces. | 2008-11-17 | 9.3 | CVE-2008-3623<br>BID<br>CONFIRM<br>APPLE |
| apple -- cups | The web interface (cgi-bin/admin.c) in CUPS before 1.3.8 uses the guest username when a user is not logged on to the web server, which makes it easier for remote attackers to bypass intended policy and conduct CSRF attacks via the (1) add and (2) cancel RSS subscription functions. | 2008-11-20 | 10.0 | CVE-2008-5184<br>MLIST<br>MISC<br>CONFIRM |

Back to top

| High Vulnerabilities | | | | |
|---|---|---|---|---|
| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
| balabit -- syslog-ng | syslog-ng does not call chdir when it calls chroot, which might allow attackers to escape the intended jail. NOTE: this is only a vulnerability when a separate vulnerability is present. | 2008-11-17 | 9.3 | CVE-2008-5110<br>MLIST<br>CONFIRM |
| boonex -- orca | PHP remote file inclusion vulnerability in layout/default/params.php in Boonex Orca 2.0 and 2.0.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the gConf[dir][layouts] parameter. | 2008-11-19 | 9.3 | CVE-2008-5167<br>BID<br>MILW0RM<br>SECUNIA |
| citrix -- deterministic_network_enhancer | dne2000.sys in Citrix Deterministic Network Enhancer (DNE) 2.21.7.233 through 3.21.7.17464, as used in (1) Cisco VPN Client, (2) Blue Coat WinProxy, and (3) SafeNet SoftRemote and HighAssurance Remote, allows local users to gain privileges via a crafted DNE_IOCTL DeviceIoControl request to the \\.\DNE device interface. | 2008-11-17 | 7.2 | CVE-2008-5121<br>CERT-VN<br>BID<br>MILW0RM<br>MISC<br>MISC<br>SECUNIA<br>SECUNIA<br>SECUNIA<br>SECUNIA |
| clientsoftware -- wincome_mpd_total | Client Software WinCom LPD Total 3.0.2.623 and earlier allows remote attackers to bypass authentication and perform administrative actions via vectors involving "simply skipping the auth stage." | 2008-11-18 | 7.5 | CVE-2008-5158<br>BID<br>BUGTRAQ<br>FRSIRT<br>SECUNIA<br>MISC<br>MISC |
| clientsoftware -- wincome_mpd_total | Integer overflow in the remote administration protocol processing in Client Software WinCom LPD Total 3.0.2.623 and earlier allows remote attackers to cause a denial of service (crash) via a large string length argument, which triggers memory corruption. | 2008-11-18 | 10.0 | CVE-2008-5159<br>BID<br>BUGTRAQ<br>FRSIRT<br>SECUNIA<br>MISC<br>MISC |
| clientsoftware -- wincom_mpd_total | Multiple buffer overflows in Client Software WinCom LPD Total 3.0.2.623 and earlier allow remote attackers to execute arbitrary code | 2008-11-20 | 9.3 | CVE-2008-5176<br>BID<br>BUGTRAQ<br>FRSIRT |

Back to top

| High Vulnerabilities | | | | |
|---|---|---|---|---|
| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
| | via (1) a long 0x02 command to the remote administration service on TCP port 13500 or (2) a long invalid control filename to LPDService.exe on TCP port 515. | | | SECUNIA<br>MISC<br>MISC |
| dcgrendel -- vmbuilder | The (1) python-vm-builder and (2) ubuntu-vm-builder implementations in VMBuilder 0.9 in Ubuntu 8.10 omit the -e option when invoking chpasswd with a root:! argument, which configures the root account with a cleartext password of ! (exclamation point) and allows attackers to bypass intended login restrictions. | 2008-11-17 | 7.2 | CVE-2008-5103<br>BID<br>SECUNIA |
| dcgrendel -- vmbuilder | Ubuntu 6.06 LTS, 7.10, 8.04 LTS, and 8.10, when installed as a virtual machine by (1) python-vm-builder or (2) ubuntu-vm-builder in VMBuilder 0.9 in Ubuntu 8.10, have ! (exclamation point) as the default root password, which allows attackers to bypass intended login restrictions. | 2008-11-17 | 7.2 | CVE-2008-5104<br>BID<br>SECUNIA |
| develop_it_easy -- news_and_article_system | Multiple SQL injection vulnerabilities in Develop It Easy News And Article System 1.4 allow remote attackers to execute arbitrary SQL commands via (1) the aid parameter to article_details.php, and the (2) username and (3) password to the admin panel (admin/index.php). | 2008-11-18 | 7.5 | CVE-2008-5131<br>BID<br>MILW0RM<br>SECUNIA |
| easysitenetwork -- riddles_website | SQL injection vulnerability in riddle.php in Riddles Website 1.2.1 allows remote attackers to execute arbitrary SQL commands via the riddleid parameter. | 2008-11-19 | 7.5 | CVE-2008-5166<br>BID<br>MILW0RM<br>SECUNIA |
| easysitenetwork -- tips_complete_website | SQL injection vulnerability in tip.php in Tips Complete Website 1.2.0 allows remote attackers to execute arbitrary SQL commands via the tipid parameter. | 2008-11-19 | 7.5 | CVE-2008-5168<br>BID<br>MILW0RM<br>SECUNIA |

Back to top

## High Vulnerabilities

| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| easysitenetwork -- drinks_complete_website | SQL injection vulnerability in drinks/drink.php in Drinks Complete Website 2.1.0 allows remote attackers to execute arbitrary SQL commands via the drinkid parameter. | 2008-11-19 | 7.5 | CVE-2008-5169<br>BID<br>MILW0RM<br>SECUNIA |
| easysitenetwork -- cheats_complete_website | SQL injection vulnerability in item.php in Cheats Complete Website 1.1.1 allows remote attackers to execute arbitrary SQL commands via the itemid parameter. | 2008-11-19 | 7.5 | CVE-2008-5170<br>BID<br>MILW0RM<br>SECUNIA |
| easysitenetwork -- jokes_complete_website | SQL injection vulnerability in joke.php in Jokes Complete Website 2.1.3 allows remote attackers to execute arbitrary SQL commands via the jokeid parameter. | 2008-11-19 | 7.5 | CVE-2008-5174<br>BID<br>MILW0RM<br>SECUNIA |
| ecryptfs -- ecryptfs_utils | The (1) ecryptfs-setup-private, (2) ecryptfs-setup-confidential, and (3) ecryptfs-setup-pam-wrapped.sh scripts in ecryptfs-utils 45 through 61 in eCryptfs place cleartext passwords on command lines, which allows local users to obtain sensitive information by listing the process. | 2008-11-20 | 7.2 | CVE-2008-5188<br>CONFIRM<br>MLIST<br>MLIST<br>MLIST<br>CONFIRM |
| ektron -- cms4000.net | SQL injection vulnerability in ContentRatingGraph.aspx in Ektron CMS400.NET 7.5.2 and earlier allows remote attackers to execute arbitrary SQL commands via the res parameter. | 2008-11-17 | 7.5 | CVE-2008-5122<br>XF<br>BID<br>MISC |
| enlightenment -- imlib2 | The load function in the XPM loader for imlib2 1.4.2, and possibly other versions, allows attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted XPM file that triggers a "pointer arithmetic error" and a heap-based buffer overflow, a different vulnerability than CVE-2008-2426. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | 2008-11-20 | 7.5 | CVE-2008-5187<br>MLIST<br>SECUNIA<br>CONFIRM |

Back to top

| High Vulnerabilities | | | | |
|---|---|---|---|---|
| **Primary Vendor -- Product** | **Description** | **Published** | **CVSS Score** | **Source & Patch Info** |
| eshop100 -- eshop100 | SQL injection vulnerability in index.php in eSHOP100 allows remote attackers to execute arbitrary SQL commands via the SUB parameter. | 2008-11-21 | 7.5 | CVE-2008-5190<br>MILW0RM<br>SECUNIA |
| eticket -- eticket | Multiple SQL injection vulnerabilities in eTicket 1.5.7 allow remote attackers to execute arbitrary SQL commands via the pri parameter to (1) index.php, (2) open.php, (3) open_raw.php, and (4) newticket.php. | 2008-11-19 | 7.5 | CVE-2008-5165<br>BID<br>CONFIRM<br>MISC<br>SECUNIA |
| geshi -- geshi | ** DISPUTED ** The set_language_path function in geshi.php in Generic Syntax Highlighter (GeSHi) before 1.0.8.1 might allow remote attackers to conduct file inclusion attacks via crafted inputs that influence the default language path ($path variable). NOTE: this issue has been disputed by a vendor, stating that only a static value is used, so this is not a vulnerability in GeSHi. Separate CVE identifiers would be created for web applications that integrate GeSHi in a way that allows control of the default language path. | 2008-11-20 | 7.5 | CVE-2008-5186<br>BID<br>CONFIRM |
| hp -- service_manager | Unspecified vulnerability in HP Service Manager (HPSM) before 7.01.71 allows remote authenticated users to execute arbitrary code via unknown vectors. | 2008-11-17 | 9.0 | CVE-2008-4415<br>BID<br>HP<br>HP |
| hp -- openvms | Stack-based buffer overflow in the Process Software MultiNet finger service (aka FINGERD) for HP OpenVMS 8.3 allows remote attackers to execute arbitrary code via a long request string. | 2008-11-17 | 10.0 | CVE-2008-5120<br>BID<br>BUGTRAQ |
| insight-tech -- yosemite_backup | Stack-based buffer overflow in the DtbClsLogin function in Yosemite Backup 8.7 allows remote attackers to (1) execute arbitrary code on a Linux platform, related to | 2008-11-20 | 10.0 | CVE-2008-5177<br>BID<br>MISC<br>MISC<br>SECUNIA |

Back to top

| High Vulnerabilities | | | | |
|---|---|---|---|---|
| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
| | libytlindtb.so; or (2) cause a denial of service (application crash) and possibly execute arbitrary code on a Windows platform, related to ytwindtb.dll; via a long username field during authentication. | | | OSVDB<br>OSVDB |
| jscape -- secure_ftp_applet | JSCAPE Secure FTP Applet 4.8.0 and earlier does not ask the user to verify a new or mismatched SSH host key, which makes it easier for remote attackers to perform man-in-the-middle attacks. | 2008-11-17 | 7.5 | CVE-2008-5124<br>XF<br>SECTRACK<br>BID<br>BUGTRAQ<br>CONFIRM<br>SECUNIA |
| karjasoft -- sami_ftp_server | Buffer overflow in KarjaSoft Sami FTP Server 2.0.x allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via a long argument to an arbitrary command, which triggers the overflow when the SamyFtp.binlog log file is viewed in the management console. NOTE: this may overlap CVE-2006-0441 and CVE-2006-2212. | 2008-11-17 | 10.0 | CVE-2008-5106<br>BID<br>BUGTRAQ |
| linux -- kernel | Stack-based buffer overflow in the hfs_cat_find_brec function in fs/hfs/catalog.c in the Linux kernel before 2.6.28-rc1 allows attackers to cause a denial of service (memory corruption or system crash) via an hfs filesystem image with an invalid catalog namelength field, a related issue to CVE-2008-4933. | 2008-11-17 | 7.8 | CVE-2008-5025<br>CONFIRM<br>MLIST<br>MLIST<br>MLIST<br>MLIST<br>MLIST<br>MLIST<br>CONFIRM |
| linux -- kernel | Buffer overflow in the lbs_process_bss function in drivers/net/wireless/libertas/scan.c in the libertas subsystem in the Linux kernel before 2.6.27.5 allows remote attackers to have an unknown impact via an "invalid beacon/probe response." | 2008-11-18 | 10.0 | CVE-2008-5134<br>CONFIRM<br>MLIST<br>CONFIRM<br>MLIST |
| memht -- memht_portal | SQL injection vulnerability in inc/ajax/ajax_rating.php in MemHT Portal 4.0.1 allows remote attackers | 2008-11-18 | 7.5 | CVE-2008-5132<br>BID<br>MILW0RM |

Back to top

| High Vulnerabilities | | | | |
|---|---|---|---|---|
| **Primary Vendor -- Product** | **Description** | **Published** | **CVSS Score** | **Source & Patch Info** |
| | to execute arbitrary SQL commands via the X-Forwarded-For HTTP header. | | | SECUNIA |
| microsoft -- .net_framework | The strong name (SN) implementation in Microsoft .NET Framework 2.0.50727 relies on the digital signature Public Key Token embedded in the pathname of a DLL file instead of the digital signature of this file itself, which makes it easier for attackers to bypass Global Assembly Cache (GAC) and Code Access Security (CAS) protection mechanisms, aka MSRC ticket MSRC8566gs. | 2008-11-17 | 10.0 | CVE-2008-5100<br>BUGTRAQ<br>MISC<br>MISC |
| opera -- opera | Heap-based buffer overflow in Opera 9.62 on Windows allows remote attackers to execute arbitrary code via a long file:// URI. | 2008-11-20 | 9.3 | CVE-2008-5178<br>BID<br>FRSIRT<br>SECUNIA<br>OSVDB<br>MILW0RM |
| optipng -- optipng | Buffer overflow in the BMP reader in OptiPNG 0.6 and 0.6.1 allows user-assisted attackers to execute arbitrary code via a crafted BMP image, related to an "array overflow." | 2008-11-17 | 9.3 | CVE-2008-5101<br>CONFIRM<br>CONFIRM |
| philboard -- philboard | SQL injection vulnerability in forum.asp in W1L3D4 Philboard 1.14 and 1.2 allows remote attackers to execute arbitrary SQL commands via the forumid parameter. NOTE: this might overlap CVE-2008-2334, CVE-2008-1939, CVE-2007-2641, or CVE-2007-0920. | 2008-11-21 | 7.5 | CVE-2008-5192<br>BID<br>MILW0RM<br>SECUNIA |
| phpblaster -- phpblaster_cms | Multiple directory traversal vulnerabilities in admin/minibb/index.php in phpBLASTER CMS 1.0 RC1, when register_globals is enabled, allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the (1) DB, (2) lang, and (3) skin | 2008-11-19 | 9.3 | CVE-2008-5171<br>MILW0RM |

Back to top

| High Vulnerabilities | | | | |
|---|---|---|---|---|
| **Primary Vendor -- Product** | **Description** | **Published** | **CVSS Score** | **Source & Patch Info** |
| | parameters. | | | |
| sebrac -- sebraccms | Multiple SQL injection vulnerabilities in SebracCMS (sbcms) 0.4 allow remote attackers to execute arbitrary SQL commands via (1) the recid parameter to cms/form/read.php, (2) the uname parameter to cms/index.php, and other unspecified vectors. | 2008-11-21 | 7.5 | CVE-2008-5195<br>BID<br>MILW0RM |
| seportal -- seportal | Multiple SQL injection vulnerabilities in SePortal 2.4 allow remote attackers to execute arbitrary SQL commands via the (1) poll_id parameter to poll.php and the (2) sp_id parameter to staticpages.php. | 2008-11-21 | 7.5 | CVE-2008-5191<br>BID<br>MILW0RM<br>SECUNIA |
| smsclient -- smsclient | mail2sms.sh in smsclient 2.0.8z allows local users to overwrite arbitrary files via a symlink attack on a (1) /tmp/header.##### or (2) /tmp/body.##### temporary file, or append data to arbitrary files via a symlink attack on the (3) /tmp/sms.log temporary file. | 2008-11-18 | 9.3 | CVE-2008-5155<br>MISC<br>MLIST |
| softvisions_software -- online_booking_manager | SQL injection vulnerability in checkavail.php in SoftVisions Software Online Booking Manager (obm) 2.2 allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2008-11-21 | 7.5 | CVE-2008-5194<br>BID<br>MILW0RM<br>SECUNIA |
| sun -- java_system_identity_manager | Unspecified vulnerability in Sun Java System Identity Manager 6.0 through 6.0 SP4, 7.0, and 7.1 allows remote attackers to access files in the local filesystem of the IDM server via unknown vectors. | 2008-11-17 | 7.8 | CVE-2008-5116<br>SUNALERT |
| testmaker -- testmaker | Unspecified vulnerability in testMaker before 3.0p16 allows remote authenticated users to execute arbitrary PHP code via unspecified attack vectors. | 2008-11-19 | 9.0 | CVE-2008-5173<br>CONFIRM |
| theratstudios -- the_rat_cms | Multiple SQL injection vulnerabilities in The Rat CMS Pre-Alpha 2 allow remote attackers to execute arbitrary SQL commands | 2008-11-19 | 7.5 | CVE-2008-5163<br>BID<br>BUGTRAQ |

**High Vulnerabilities**

| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | via the id parameter to (1) viewarticle.php and (2) viewarticle2.php. | | | |
| trend_micro -- serverprotect | Unspecified vulnerability in Trend Micro ServerProtect 5.7 and 5.58 allows remote attackers to execute arbitrary code via vectors related to obtaining "administrative access to the RPC interface." | 2008-11-17 | 10.0 | CVE-2006-5268<br>XF<br>BID<br>ISS<br>FRSIRT<br>SECUNIA<br>MISC |
| trend_micro -- serverprotect | Heap-based buffer overflow in an unspecified procedure in Trend Micro ServerProtect 5.7 and 5.58 allows remote attackers to execute arbitrary code via unknown vectors, probably related to an RPC interface. | 2008-11-17 | 10.0 | CVE-2006-5269<br>XF<br>BID<br>ISS<br>FRSIRT<br>SECUNIA<br>MISC |
| trend_micro -- serverprotect | Heap-based buffer overflow in an unspecified procedure in Trend Micro ServerProtect 5.7 and 5.58 allows remote attackers to execute arbitrary code via unknown vectors, possibly related to a read operation over RPC. | 2008-11-17 | 10.0 | CVE-2007-0072<br>XF<br>BID<br>ISS<br>FRSIRT<br>SECUNIA<br>MISC |
| trend_micro -- serverprotect | Heap-based buffer overflow in an unspecified procedure in Trend Micro ServerProtect 5.7 and 5.58 allows remote attackers to execute arbitrary code via unknown vectors, possibly related to a file read operation over RPC. | 2008-11-17 | 10.0 | CVE-2007-0073<br>XF<br>BID<br>ISS<br>FRSIRT<br>SECUNIA<br>MISC |
| trend_micro -- serverprotect | Heap-based buffer overflow in an unspecified procedure in Trend Micro ServerProtect 5.7 and 5.58 allows remote attackers to execute arbitrary code via unknown vectors, possibly related to a folder read operation over RPC. | 2008-11-17 | 10.0 | CVE-2007-0074<br>XF<br>BID<br>ISS<br>FRSIRT<br>SECUNIA<br>MISC |
| trend_micro -- serverprotect | Heap-based buffer overflow in an unspecified procedure in Trend Micro ServerProtect 5.7 and 5.58 allows remote attackers to execute arbitrary code via unknown vectors, possibly related to the product's | 2008-11-17 | 10.0 | CVE-2008-0012<br>XF<br>BID<br>ISS<br>FRSIRT<br>SECUNIA |

Back to top

## High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | configuration, a different vulnerability than CVE-2008-0013 and CVE-2008-0014. | | | MISC |
| trend_micro -- serverprotect | Heap-based buffer overflow in an unspecified procedure in Trend Micro ServerProtect 5.7 and 5.58 allows remote attackers to execute arbitrary code via unknown vectors, possibly related to the product's configuration, a different vulnerability than CVE-2008-0012 and CVE-2008-0014. | 2008-11-17 | 10.0 | CVE-2008-0013<br>XF<br>BID<br>ISS<br>FRSIRT<br>SECUNIA<br>MISC |
| trend_micro -- serverprotect | Heap-based buffer overflow in an unspecified procedure in Trend Micro ServerProtect 5.7 and 5.58 allows remote attackers to execute arbitrary code via unknown vectors, possibly related to the product's configuration, a different vulnerability than CVE-2008-0012 and CVE-2008-0013. | 2008-11-17 | 10.0 | CVE-2008-0014<br>XF<br>BID<br>ISS<br>FRSIRT<br>SECUNIA<br>MISC |
| visicommedia -- aceftp | Directory traversal vulnerability in the FTP client in AceFTP Freeware 3.80.3 and AceFTP Pro 3.80.3 allows remote FTP servers to create or overwrite arbitrary files via a .. (dot dot) in a response to a LIST command, a related issue to CVE-2002-1345. | 2008-11-19 | 9.3 | CVE-2008-5175<br>FRSIRT<br>MISC<br>SECUNIA |

Back to top

## Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| abottoms -- mayavi | test_parser.py in mayavi 1.5 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/err.log temporary file. | 2008-11-18 | 6.9 | CVE-2008-5151<br>MISC<br>MLIST |
| adobe -- adobe_air | Unspecified vulnerability in Adobe AIR 1.1 and earlier allows context-dependent attackers to execute untrusted JavaScript in an AIR application via unknown attack | 2008-11-17 | 6.8 | CVE-2008-5108<br>CONFIRM |

Back to top

| Medium Vulnerabilities | | | | |
|---|---|---|---|---|
| **Primary Vendor -- Product** | **Description** | **Published** | **CVSS Score** | **Source & Patch Info** |
| | vectors. | | | |
| apple -- cups | cupsd in CUPS before 1.3.8 allows local users, and possibly remote attackers, to cause a denial of service (daemon crash) by adding a large number of RSS Subscriptions, which triggers a NULL pointer dereference. NOTE: this issue can be triggered remotely by leveraging CVE-2008-5184. | 2008-11-20 | 4.3 | CVE-2008-5183<br>CONFIRM<br>MLIST<br>MLIST<br>MISC |
| aucko -- libncbi6 | fwd_check.sh in libncbi6 6.1.20080302 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/##### temporary file. | 2008-11-18 | 6.9 | CVE-2008-5149<br>MISC<br>MLIST |
| bkleineidam -- libpam_mount | passwdehd in libpam-mount 0.43 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/passwdehd.##### temporary file. | 2008-11-18 | 6.9 | CVE-2008-5138<br>MLIST |
| boutikone -- boutikone_cms | Cross-site scripting (XSS) vulnerability in search.php in BoutikOne CMS allows remote attackers to inject arbitrary web script or HTML via the search_query parameter. | 2008-11-17 | 4.3 | CVE-2008-5126<br>XF<br>BID<br>SECUNIA<br>MISC |
| castillocentral -- ccleague | SQL injection vulnerability in admin.php in CCleague Pro 1.2 allows remote attackers to execute arbitrary SQL commands via the u parameter. | 2008-11-17 | 6.8 | CVE-2008-5123<br>XF<br>BID<br>MILW0RM<br>SECUNIA |
| castillocentral -- ccleague | admin.php in CCleague Pro 1.2 allows remote attackers to bypass authentication by setting the type cookie value to admin. | 2008-11-17 | 6.8 | CVE-2008-5125<br>XF<br>BID<br>MILW0RM<br>SECUNIA |
| dann_frazier -- flamethrower | flamethrower in flamethrower 0.1.8 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/multicast.tar.##### temporary file. | 2008-11-18 | 6.9 | CVE-2008-5141<br>MLIST |
| dann_frazier -- systemimager-server | si_mkbootserver in systemimager-server 3.6.3 allows local users to overwrite arbitrary files | 2008-11-18 | 6.9 | CVE-2008-5156<br>MISC<br>MLIST |

Back to top

**Medium Vulnerabilities**

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | via a symlink attack on a (1) /tmp/*.inetd.conf or (2) /tmp/pxe.conf.*.tmp temporary file. | | | |
| debian -- os-prober | ** DISPUTED ** os-prober in os-prober 1.17 allows local users to overwrite arbitrary files via a symlink attack on the (1) /tmp/mounted-map or (2) /tmp/raided-map temporary file. NOTE: the vendor disputes this issue, stating "the insecure code path should only ever run inside a d-i environment, which has no non-root users." | 2008-11-18 | 6.2 | CVE-2008-5135<br>MLIST<br>MLIST |
| debian -- mailscanner | trend-autoupdate.new in mailscanner 4.55.10 allows local users to overwrite arbitrary files via a symlink attack on a (1) /tmp/opr.ini.##### or (2) /tmp/lpt*.zip temporary file. | 2008-11-18 | 6.9 | CVE-2008-5140<br>MLIST |
| debian -- ltp | ltpmenu in ltp 20060918 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/runltp.mainmenu.##### temporary file. | 2008-11-18 | 6.9 | CVE-2008-5145<br>MLIST |
| erl_wustl -- ctn | add-accession-numbers in ctn 3.0.6 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/accession temporary file. | 2008-11-18 | 6.9 | CVE-2008-5146<br>MISC<br>MLIST |
| federico_di_gregorio -- nvidia-cg-toolkit | nvidia-cg-toolkit-installer in nvidia-cg-toolkit 2.0.0015 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/nvidia-cg-toolkit-manifest temporary file. | 2008-11-18 | 6.9 | CVE-2008-5144<br>MLIST |
| forumsoftware -- yazd_forum_software | Multiple cross-site scripting (XSS) vulnerabilities in Yazd Forum Software 3.x allow remote attackers to inject arbitrary web script or HTML via the (1) q parameter to (a) search.jsp, and the (2) msg parameter to (b) error.jsp and (c) userAccount.jsp. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | 2008-11-19 | 4.3 | CVE-2008-5172<br>SECUNIA |

Back to top

| Medium Vulnerabilities | | | | |
|---|---|---|---|---|
| **Primary Vendor -- Product** | **Description** | **Published** | **CVSS Score** | **Source & Patch Info** |
| freebsd -- freebsd-sendpr | sendbug in freebsd-sendpr 3.113+5.3 on Debian GNU/Linux allows local users to overwrite arbitrary files via a symlink attack on a /tmp/pr.##### temporary file. | 2008-11-18 | 6.9 | CVE-2008-5142<br>MLIST |
| geda -- gnetlist | sch2eaglepos.sh in geda-gnetlist 1.4.0 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/##### temporary file. | 2008-11-18 | 6.9 | CVE-2008-5148<br>MISC<br>MLIST |
| geshi -- geshi | The highlighting functionality in geshi.php in GeSHi before 1.0.8 allows remote attackers to cause a denial of service (infinite loop) via an XML sequence containing an opening delimiter without a closing delimiter, as demonstrated using "<". | 2008-11-20 | 5.0 | CVE-2008-5185<br>MLIST<br>CONFIRM |
| holloway -- docvert | test-pipe-to-pyodconverter.org.sh in docvert 2.4 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/outer.odt temporary file. | 2008-11-18 | 6.9 | CVE-2008-5147<br>MISC<br>MLIST |
| javier_fernandez -- jailer | updatejail in jailer 0.4 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/#####.updatejail temporary file. | 2008-11-18 | 6.9 | CVE-2008-5139<br>MLIST |
| jose_carlos_medeiros -- maildirsync | sample.sh in maildirsync 1.1 allows local users to append data to arbitrary files via a symlink attack on a /tmp/maildirsync-*.#####.log temporary file. | 2008-11-18 | 6.9 | CVE-2008-5150<br>MISC<br>MLIST |
| karjasoft -- sami_ftp_server | KarjaSoft Sami FTP Server 2.0.x allows remote attackers to cause a denial of service (daemon crash or hang) via certain (1) APPE, (2) CWD, (3) DELE, (4) MKD, (5) RMD, (6) RETR, (7) RNFR, (8) RNTO, (9) SIZE, and (10) STOR commands. | 2008-11-17 | 5.0 | CVE-2008-5105<br>BID<br>BUGTRAQ |
| koeniglich -- p3nfs | bluetooth.rc in p3nfs 5.19 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/blue.log temporary file. | 2008-11-18 | 6.9 | CVE-2008-5154<br>MISC<br>MLIST |
| ldrolez -- tkusr | tkusr in tkusr 0.82 allows local users to overwrite arbitrary files via a | 2008-11-18 | 6.9 | CVE-2008-5136<br>MLIST |

Back to top

**Medium Vulnerabilities**

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | symlink attack on the /tmp/tkusr.pgm temporary file. | | | |
| linux -- kernel | The inotify functionality in Linux kernel 2.6 before 2.6.28-rc5 might allow local users to gain privileges via unknown vectors related to race conditions in inotify watch removal and umount. | 2008-11-20 | 6.9 | CVE-2008-5182<br>CONFIRM |
| microsoft -- windows | The LDAP server in Active Directory in Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2 responds differently to a failed bind attempt depending on whether the user account exists and is permitted to login, which allows remote attackers to enumerate valid usernames via a series of LDAP bind requests, as demonstrated by ldapuserenum. | 2008-11-17 | 5.0 | CVE-2008-5112<br>BID<br>MISC<br>MISC |
| microsoft -- office_communications_server<br>microsoft -- office_communicator<br>microsoft -- windows_live_messenger | Unspecified vulnerability in Microsoft Office Communications Server (OCS), Office Communicator, and Windows Live Messenger allows remote attackers to cause a denial of service (crash) via a crafted Real-time Transport Control Protocol (RTCP) receiver report packet. | 2008-11-20 | 5.0 | CVE-2008-5179<br>XF<br>MISC<br>BID |
| microsoft -- office_communicator | Microsoft Communicator allows remote attackers to cause a denial of service (memory consumption) via a large number of SIP INVITE requests, which trigger the creation of many sessions. | 2008-11-20 | 5.0 | CVE-2008-5180<br>XF<br>MISC |
| microsoft -- office_communicator | Microsoft Communicator allows remote attackers to cause a denial of service (application or device outage) via instant messages containing large numbers of emoticons. | 2008-11-20 | 5.0 | CVE-2008-5181<br>XF<br>MISC |
| mohammed_sameer -- multi-gnome-terminal | mgt-helper in multi-gnome-terminal 1.6.2 allows local users to overwrite arbitrary files via a symlink attack on a (1) /tmp/*.debug or (2) /tmp/*.env temporary file. | 2008-11-18 | 6.9 | CVE-2008-5143<br>MLIST |

Back to top

**Medium Vulnerabilities**

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| moodle -- moodle | spell-check-logic.cgi in Moodle 1.8.2 allows local users to overwrite arbitrary files via a symlink attack on the (1) /tmp/spell-check-debug.log, (2) /tmp/spell-check-before, or (3) /tmp/spell-check-after temporary file. | 2008-11-18 | 6.9 | CVE-2008-5153<br>MISC<br>MLIST |
| myserver -- myserver | Unspecified vulnerability in MyServer 0.8.11 allows remote attackers to cause a denial of service (daemon crash) via multiple invalid requests with the HTTP GET, DELETE, OPTIONS, and possibly other methods, related to a "204 No Content error." | 2008-11-18 | 5.0 | CVE-2008-5160<br>BID<br>MILW0RM |
| ocean12_technologies -- contact_manager | Ocean12 Contact Manager Pro 1.02 stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain sensitive information via a direct request to o12con.mdb. | 2008-11-18 | 5.0 | CVE-2008-5127<br>XF<br>SECUNIA<br>MISC |
| ocean12_technologies -- membership_manager_pro | Ocean12 Membership Manager Pro stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain sensitive information via a direct request to o12member.mdb. | 2008-11-18 | 5.0 | CVE-2008-5128<br>XF<br>SECUNIA<br>MISC |
| ocean12_technologies -- poll_manager | Ocean12 Poll Manager Pro 1.00 stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain sensitive information via a direct request to o12poll.mdb. | 2008-11-18 | 5.0 | CVE-2008-5129<br>XF<br>SECUNIA<br>MISC |
| ocean12_technologies -- calendar_manager | Ocean12 Calendar Manager Gold 2.04 stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain sensitive information via a direct request to o12cal.mdb. | 2008-11-18 | 5.0 | CVE-2008-5130<br>XF<br>SECUNIA<br>MISC |

Back to top

**Medium Vulnerabilities**

| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| peter_s_galbraith -- mh-book | inmail-show in mh-book 200605 allows local users to overwrite arbitrary files via a symlink attack on a (1) /tmp/inmail#####.log or (2) /tmp/inmail#####.stdin temporary file. | 2008-11-18 | 6.9 | CVE-2008-5152<br>MISC<br>MLIST |
| philboard -- philboard | Cross-site scripting (XSS) vulnerability in search.asp in W1L3D4 Philboard 1.14 and 1.2 allows remote attackers to inject arbitrary web script or HTML via the searchterms parameter. NOTE: this might overlap CVE-2007-4024. | 2008-11-21 | 4.3 | CVE-2008-5193<br>BID<br>MILW0RM<br>SECUNIA |
| rpath -- initscripts | rc.sysinit in initscripts 8.12-8.21 and 8.56.15-0.1 on rPath allows local users to delete arbitrary files via a symlink attack on a directory under (1) /var/lock or (2) /var/run. NOTE: this issue exists because of a race condition in an incorrect fix for CVE-2008-3524. NOTE: exploitation may require an unusual scenario in which rc.sysinit is executed other than at boot time. | 2008-11-17 | 6.9 | CVE-2008-4832<br>CONFIRM<br>CONFIRM |
| ruby_on_rails -- ruby_on_rails | CRLF injection vulnerability in Ruby on Rails before 2.0.5 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via a crafted URL to the redirect_to function. | 2008-11-21 | 5.0 | CVE-2008-5189<br>BID |
| scripts4profit -- dxshopcart | Cross-site scripting (XSS) vulnerability in search.php in Scripts4Profit DXShopCart 4.30mc allows remote attackers to inject arbitrary web script or HTML via the keyword parameter. | 2008-11-17 | 4.3 | CVE-2008-5119<br>XF<br>BID<br>FULLDISC |
| sun -- java_system_messaging_server | Cross-site scripting (XSS) vulnerability in Sun Java System Messaging Server 6.2 and 6.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2007-2904. | 2008-11-17 | 4.3 | CVE-2008-5098<br>SUNALERT |

Back to top

| Medium Vulnerabilities | | | | |
|---|---|---|---|---|
| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
| sun -- logical_domain_manager | Sun Logical Domain Manager (aka LDoms Manager or ldm) 1.0 through 1.0.3 displays the value of the OpenBoot PROM (OBP) security-password variable in cleartext, which allows local users to bypass the SPARC firmware's password protection, and gain privileges or obtain data access, via the "ldm ls -l" command, a different vulnerability than CVE-2008-4992. | 2008-11-17 | 4.6 | CVE-2008-5099<br>CONFIRM<br>CONFIRM |
| sun -- opensolaris<br>sun -- solaris | Unspecified vulnerability in the socket function in Sun Solaris 10 and OpenSolaris snv_57 through snv_91, when InfiniBand hardware is not installed, allows local users to cause a denial of service (panic) via unknown vectors, related to the socksdpv_close function. | 2008-11-17 | 4.7 | CVE-2008-5111<br>SUNALERT |
| sun -- java_system_identity_manager | Cross-site request forgery (CSRF) vulnerability in Sun Java System Identity Manager 6.0 through 6.0 SP4, 7.0, and 7.1 allows remote attackers to obtain access to the Administrator account via unspecified vectors. | 2008-11-17 | 6.8 | CVE-2008-5115<br>SUNALERT |
| sun -- java_system_identity_manager | Sun Java System Identity Manager 6.0 through 6.0 SP4, 7.0, and 7.1 allows remote attackers to inject frames from arbitrary web sites and conduct phishing attacks via unspecified vectors, related to "frame injection." | 2008-11-17 | 4.3 | CVE-2008-5118<br>XF<br>BID<br>FRSIRT<br>SUNALERT<br>SECUNIA |
| sun -- opensolaris<br>sun -- solaris | ipnat in IP Filter in Sun Solaris 10 and OpenSolaris before snv_96, when running on a DNS server with Network Address Translation (NAT) configured, improperly changes the source port of a packet when the destination port is the DNS port, which allows remote attackers to bypass an intended CVE-2008-1447 protection mechanism and spoof the responses to DNS queries sent by named. | 2008-11-18 | 5.8 | CVE-2008-5133<br>SUNALERT |

Back to top

| Medium Vulnerabilities | | | | |
|---|---|---|---|---|
| **Primary Vendor -- Product** | **Description** | **Published** | **CVSS Score** | **Source & Patch Info** |
| theratstudios -- the_rat_cms | Multiple cross-site scripting (XSS) vulnerabilities in The Rat CMS Pre-Alpha 2 allow remote attackers to inject arbitrary web script or HTML via the (1) id parameter to (a) viewarticle.php and (b) viewarticle2.php and the (2) PATH_INFO to viewarticle.php. | 2008-11-19 | 4.3 | CVE-2008-5164<br>BID<br>BUGTRAQ |
| tkman -- tkman | tkman in tkman 2.2 allows local users to overwrite arbitrary files via a symlink attack on a (1) /tmp/tkman##### or (2) /tmp/ll temporary file. | 2008-11-18 | 6.9 | CVE-2008-5137<br>MLIST |
| wordpress -- wordpress | WordPress 2.6.3 relies on the REQUEST superglobal array in certain dangerous situations, which makes it easier for remote attackers to conduct delayed and persistent cross-site request forgery (CSRF) attacks via crafted cookies, as demonstrated by attacks that (1) delete user accounts or (2) cause a denial of service (loss of application access). NOTE: this issue relies on the presence of an independent vulnerability that allows cookie injection. | 2008-11-17 | 4.0 | CVE-2008-5113<br>MLIST<br>CONFIRM |
| yann_dirson -- tau | tau 2.16.4 allows local users to overwrite arbitrary files via a symlink attack on a (1) /tmp/makefile.tau.*.##### or (2) /tmp/makefile.tau*.##### temporary file, related to the (a) tau_cxx, (b) tau_f90, and (c) tau_cc scripts. | 2008-11-18 | 6.9 | CVE-2008-5157<br>MISC<br>MLIST |
| zope -- zope | PythonScripts in Zope 2 2.11.2 and earlier, as used in Conga and other products, allows remote authenticated users to cause a denial of service (resource consumption or application halt) via certain (1) raise or (2) import statements. | 2008-11-17 | 4.0 | CVE-2008-5102<br>CONFIRM |

Back to top

| Low Vulnerabilities | | | | |
|---|---|---|---|---|
| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |

| | | | | |
|---|---|---|---|---|
| apple -- safari | Apple Safari before 3.2 does not properly prevent caching of form data for form fields that have autocomplete disabled, which allows local users to obtain sensitive information by reading the browser's page cache. | 2008-11-17 | 1.9 | CVE-2008-3644<br>BID<br>CONFIRM<br>APPLE |
| citrix -- desktop_server<br>citrix -- presentation_server | The installation process for Citrix Presentation Server 4.5 and Desktop Server 1.0, when MSI logging is enabled, stores database credentials in MSI log files, which allows local users to obtain these credentials by reading the log files. | 2008-11-17 | 1.9 | CVE-2008-5107<br>BID<br>FRSIRT<br>CONFIRM |
| openssh -- openssh<br>ssh -- tectia_client<br>ssh -- tectia_connector<br>ssh -- tectia_connectsecure<br>ssh -- tectia_server | Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors. | 2008-11-19 | 2.6 | CVE-2008-5161<br>XF<br>CONFIRM<br>SECTRACK<br>SECTRACK<br>BID<br>FRSIRT<br>FRSIRT<br>MISC<br>SECUNIA<br>SECUNIA<br>OSVDB<br>MISC |
| sun -- java_system_identity_manager | Open redirect vulnerability in Sun Java System Identity Manager 6.0 through 6.0 SP4, 7.0, and 7.1 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. | 2008-11-17 | 0.0 | CVE-2008-5117<br>SUNALERT |
| Back to top | | | | |