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<br>Vendor -- Product | Description | Published | CVSS Score | Sourc<br>Patch |
|---|---|---|---|---|
| 1st_news -- 4_professional | SQL injection vulnerability in products.php in 1st News 4 Professional (PR 1) allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R |
| adobe -- pagemaker | Stack-based buffer overflow in AldFs32.dll in Adobe PageMaker 7.0.1 and 7.0.2 allows user-assisted remote attackers to execute arbitrary code via a malformed .PMD file, related to "Key Strings," a different vulnerability than CVE-2007-5169 and CVE-2007-5394. | 2008-10-31 | 9.3 | CVE-200<br>BID<br>CONFIR |
| adobe -- acrobat<br>adobe -- reader | Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a PDF file that calls the util.printf JavaScript function with a crafted format string argument, a related issue to CVE-2008-1104. | 2008-11-04 | 9.3 | CVE-200<br>MISC<br>BID<br>BUGTRA<br>BUGTRA<br>BUGTRA<br>MISC<br>CONFIR<br>MISC<br>SECUNI |

Back to top

### High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Sourc Patch I |
|---|---|---|---|---|
| adobe -- acrobat<br>adobe -- reader | Array index error in Adobe Reader and Acrobat, and the Explorer extension (aka AcroRd32Info), 8.1.2, 8.1.1, and earlier allows remote attackers to execute arbitrary code via a crafted PDF document that triggers an out-of-bounds write, related to parsing of Type 1 fonts. | 2008-11-05 | 9.3 | CVE-200<br>CONFIR |
| adobe -- acrobat<br>adobe -- reader | Adobe Reader and Acrobat 8.1.2 and earlier allow remote attackers to execute arbitrary code via a crafted PDF document that (1) performs unspecified actions on a Collab object that trigger memory corruption, related to a GetCosObj method; or (2) contains a malformed PDF object that triggers memory corruption during parsing. | 2008-11-05 | 9.3 | CVE-200<br>CONFIR |
| adobe -- acrobat<br>adobe -- reader | Unspecified vulnerability in a JavaScript method in Adobe Reader and Acrobat 8.1.2 and earlier allows remote attackers to execute arbitrary code via unknown vectors, related to an "input validation issue." | 2008-11-05 | 9.3 | CVE-200<br>CONFIR |
| adobe -- acrobat<br>adobe -- reader | Untrusted search path vulnerability in Adobe Reader and Acrobat 8.1.2 and earlier on Unix and Linux allows attackers to gain privileges via a Trojan Horse program in an unspecified directory that is associated with an insecure RPATH. | 2008-11-05 | 7.5 | CVE-200<br>CONFIR |
| adobe -- acrobat<br>adobe -- reader | The Download Manager in Adobe Acrobat Professional and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a crafted PDF document that calls an AcroJS function with a long string argument, triggering heap corruption. | 2008-11-05 | 9.3 | CVE-200<br>CONFIR |
| chattaitaliano -- istant-replay | PHP remote file inclusion vulnerability in read.php in Chattaitaliano Istant-Replay allows remote attackers to execute arbitrary PHP code via a URL in the data parameter. | 2008-11-03 | 7.5 | CVE-200<br>XF<br>BID<br>BUGTRA |
| chipmunk_scripts -- chipmunk_cms | board/admin/reguser.php in Chipmunk CMS 1.3 allows remote attackers to bypass authentication and gain | 2008-11-04 | 7.5 | CVE-200<br>XF<br>MILW0R |

Back to top

**High Vulnerabilities**

| Primary Vendor -- Product | Description | Published | CVSS Score | Sourc Patch I |
|---|---|---|---|---|
| | administrator privileges via a direct request. NOTE: some of these details are obtained from third party information. | | | SECUNI |
| cisco -- catos<br>cisco -- ios | Unspecified vulnerability in the VLAN Trunking Protocol (VTP) implementation on Cisco IOS and CatOS, when the VTP operating mode is not transparent, allows remote attackers to cause a denial of service (device reload or hang) via a crafted VTP packet. | 2008-11-06 | 7.1 | CVE-200<br>XF<br>BID<br>CISCO<br>SECTRA |
| comingchina -- u-mail_webmail_server | webmail/modules/filesystem/edit.php in U-Mail Webmail server 4.91 allows remote attackers to overwrite arbitrary files via an absolute pathname in the path parameter and arbitrary content in the content parameter. NOTE: this can be leveraged for code execution by writing to a file under the web document root. | 2008-11-05 | 9.0 | CVE-200<br>XF<br>BID<br>BUGTRA |
| dev!l's -- clanportal | SQL injection vulnerability in index.php in deV!L'z Clanportal (DZCP) 1.4.9.6 and earlier allows remote attackers to execute arbitrary SQL commands via the users parameter in an addbuddy operation in a buddys action. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R<br>SECUNI |
| djvu -- activex_control_for_microsoft_office_2000 | Buffer overflow in the DjVu ActiveX Control 3.0 for Microsoft Office (DjVu_ActiveX_MSOffice.dll) allows remote attackers to execute arbitrary code via a long (1) ImageURL property, and possibly the (2) Mode, (3) Page, or Zoom properties. | 2008-11-04 | 9.3 | CVE-200<br>BID<br>MILW0R<br>FRSIRT |
| ec-cube -- ec-cube | SQL injection vulnerability in LOCKON CO.,LTD. EC-CUBE 2.3.0 and earlier, 1.4.7 and earlier, and 1.5.0-beta2 and earlier; and Community Edition 1.3.5 and earlier allows remote attackers to execute arbitrary SQL commands via the parameter. | 2008-11-06 | 7.5 | CVE-200<br>CONFIR<br>JVNDB<br>JVN |
| hp -- tru64 | Unspecified vulnerability in the AdvFS showfile command in HP Tru64 UNIX 5.1B-3 and 5.1B-4 allows local users | 2008-11-07 | 7.2 | CVE-200<br>BID |

Back to top

**High Vulnerabilities**

| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Sourc<br>Patch |
|---|---|---|---|---|
| | to gain privileges via unspecified vectors. | | | |
| linux -- kernel | Buffer overflow in the hfsplus_find_cat function in fs/hfsplus/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 hfsplus filesystem image with an invalid catalog namelength field, related to the hfsplus_cat_build_key_uni function. | 2008-11-05 | 7.8 | CVE-200<br>BID |
| linux -- kernel | The hfsplus_block_allocate function in fs/hfsplus/bitmap.c in the Linux kernel before 2.6.28-rc1 does not check a certain return value before calling kmap, which allows attackers to cause a denial of service (system crash) via a crafted hfsplus filesystem image. | 2008-11-05 | 7.8 | CVE-200<br>MLIST<br>SECUNI<br>CONFIR<br>CONFIR |
| linux -- kernel<br>ubuntu -- linux_kernel | Multiple buffer overflows in the ndiswrapper module 1.53 for the Linux kernel 2.6 allow remote attackers to execute arbitrary code by sending packets over a local wireless network that specify long ESSIDs. | 2008-11-06 | 8.3 | CVE-200<br>CONFIR<br>CONFIR<br>UBUNT<br>MLIST<br>SECUNI<br>CONFIR<br>CONFIR |
| maran -- php_shop | SQL injection vulnerability in prod.php in Maran PHP Shop allows remote attackers to execute arbitrary SQL commands via the cat parameter, a different vector than CVE-2008-4880. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R |
| maran -- php_shop | SQL injection vulnerability in prodshow.php in Maran PHP Shop allows remote attackers to execute arbitrary SQL commands via the id parameter, a different vector than CVE-2008-4879. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R |
| mw6_technologies -- aztec_activex | Multiple insecure method vulnerabilities in MW6 Technologies Aztec ActiveX control (AZTECLib.MW6Aztec, Aztec.dll) 3.0.0.1 allow remote attackers to overwrite arbitrary files via a full pathname argument to the (1) | 2008-11-04 | 9.0 | CVE-200<br>MILW0R<br>SECUNI |

Back to top

**High Vulnerabilities**

| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Sourc<br>Patch I |
|---|---|---|---|---|
| | SaveAsBMP and (2) SaveAsWMF methods. | | | |
| mw6_technologies -- 1d_barcode_decoder_activex | Multiple insecure method vulnerabilities in MW6 Technologies 1D Barcode ActiveX control (BARCODELib.MW6Barcode, Barcode.dll) 3.0.0.1 allow remote attackers to overwrite arbitrary files via a full pathname argument to the (1) SaveAsBMP and (2) SaveAsWMF methods. | 2008-11-04 | 9.0 | CVE-200<br>MILW0R<br>SECUNI |
| mw6_technologies -- datamatrix_activex | Multiple insecure method vulnerabilities in MW6 Technologies DataMatrix ActiveX control (DATAMATRIXLib.MW6DataMatrix, DataMatrix.dll) 3.0.0.1 allow remote attackers to overwrite arbitrary files via a full pathname argument to the (1) SaveAsBMP and (2) SaveAsWMF methods. | 2008-11-04 | 9.0 | CVE-200<br>MILW0R<br>SECUNI |
| mw6_technologies -- pdf417_activex | Multiple insecure method vulnerabilities in MW6 Technologies PDF417 ActiveX control (MW6PDF417Lib.PDF417, MW6PDF417.dll) 3.0.0.1 allow remote attackers to overwrite arbitrary files via a full pathname argument to the (1) SaveAsBMP and (2) SaveAsWMF methods. | 2008-11-04 | 9.0 | CVE-200<br>MILW0R<br>SECUNI |
| netrisk -- netrisk | SQL injection vulnerability in index.php in NetRisk 2.0 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter in a (1) profile or (2) game page. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R |
| python_software_foundation -- python | Multiple integer overflows in imageop.c in the imageop module in Python 1.5.2 through 2.5.1 allow context-dependent attackers to break out of the Python VM and execute arbitrary code via large integer values in certain arguments to the crop function, leading to a buffer overflow, a different vulnerability than CVE-2007-4965 and CVE-2008-1679. | 2008-10-31 | 7.5 | CVE-200<br>BID<br>MLIST<br>MLIST<br>CONFIR<br>CONFIR<br>MISC |

Back to top

**High Vulnerabilities**

| Primary Vendor -- Product | Description | Published | CVSS Score | Sourc Patch I |
|---|---|---|---|---|
| rs_maxsoft -- fotogalerie | SQL injection vulnerability in popup_img.php in the fotogalerie module in RS MAXSOFT allows remote attackers to execute arbitrary SQL commands via the fotoID parameter. NOTE: this issue was disclosed by an unreliable researcher, so it might be incorrect. | 2008-11-03 | 7.5 | CVE-200<br>XF<br>BID<br>MILW0R |
| scripts_frenzy -- article_publisher_pro | SQL injection vulnerability in admin/admin.php in Article Publisher Pro 1.5 allows remote attackers to execute arbitrary SQL commands via the username parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>SECUNI<br>MILW0R |
| scripts_frenzy -- article_publisher_pro | SQL injection vulnerability in contact_author.php in Article Publisher Pro 1.5 allows remote attackers to execute arbitrary SQL commands via the userid parameter. | 2008-11-03 | 7.5 | CVE-200<br>SECUNI<br>MILW0R |
| smarty -- smarty | The _expand_quoted_text function in libs/Smarty_Compiler.class.php in Smarty 2.6.20 r2797 and earlier allows remote attackers to execute arbitrary PHP code via vectors related to templates and a \ (backslash) before a dollar-sign character. | 2008-10-31 | 7.5 | CVE-200<br>MLIST<br>MISC<br>SECUNI |
| sun -- java_web_start | The BasicService in Sun Java Web Start allows remote attackers to execute arbitrary programs on a client machine via a file:// URL argument to the showDocument method. | 2008-11-03 | 10.0 | CVE-200<br>XF<br>BID<br>BUGTRA<br>BUGTRA |
| ubuntu -- linux | Unspecified vulnerability in enscript before 1.6.4 in Ubuntu Linux 6.06 LTS, 7.10, 8.04 LTS, and 8.10 has unknown impact and attack vectors, possibly related to a buffer overflow. | 2008-11-04 | 9.3 | CVE-200<br>UBUNTU<br>SECUNI |
| visagesoft -- expert_pdf_viewer_activex | Insecure method vulnerability in VISAGESOFT eXPert PDF Viewer X ActiveX control (VSPDFViewerX.ocx) 3.0.990.0 allows remote attackers to overwrite arbitrary files via a full pathname to the savePageAsBitmap method. | 2008-11-04 | 9.4 | CVE-200<br>MILW0R<br>SECUNI |
| w1n78 -- lyrics | SQL injection vulnerability in lyrics_song.php in the Lyrics (lyrics_menu) plugin for e107 allows remote attackers to execute arbitrary | 2008-11-03 | 7.5 | CVE-200<br>MISC<br>BID<br>MILW0R |

Back to top

**High Vulnerabilities**

| Primary<br>Vendor -- Product | Description | Published | CVSS Score | Source<br>Patch |
|---|---|---|---|---|
| | SQL commands via the l_id parameter. | | | |
| yourfreeworld -- reminder_service_script | SQL injection vulnerability in tr.php in YourFreeWorld Reminder Service Script allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R<br>SECUNI |
| yourfreeworld -- autoresponder_hosting_script | SQL injection vulnerability in tr.php in YourFreeWorld Autoresponder Hosting Script allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R<br>SECUNI |
| yourfreeworld -- blog_blaster_script | SQL injection vulnerability in tr.php in YourFreeWorld Blog Blaster Script allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R<br>SECUNI |
| yourfreeworld -- classifieds_hosting_script | SQL injection vulnerability in tr.php in YourFreeWorld Classifieds Hosting Script allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R |
| yourfreeworld -- scrolling_text_ads_script | SQL injection vulnerability in tr1.php in YourFreeWorld Scrolling Text Ads Script allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R |
| yourfreeworld -- shopping_cart_script | SQL injection vulnerability in index.php in YourFreeWorld Shopping Cart Script allows remote attackers to execute arbitrary SQL commands via the c parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R<br>SECUNI |
| yourfreeworld -- downline_builder_script | SQL injection vulnerability in tr.php in YourFreeWorld Downline Builder allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R<br>FRSIRT |
| yourfreeworld -- classifieds_blaster_script | SQL injection vulnerability in tr.php in YourFreeWorld Classifieds Blaster Script allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2008-11-03 | 7.5 | CVE-200<br>BID<br>MILW0R<br>FRSIRT |

Back to top

| Medium Vulnerabilities | | | |
|---|---|---|---|
| Primary<br>Vendor -- Product | Description | Published | CV<br>Sco |
| | senddoc in OpenOffice.org (OOo) 2.4.1 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/log.obr.##### temporary file. | 2008-11-05 | 6. |
| adobe -- acrobat<br>adobe -- reader | Unspecified vulnerability in the Download Manager in Adobe Reader 8.1.2 and earlier on Windows allows remote attackers to change Internet Security options on a client machine via unknown vectors. | 2008-11-05 | 4. |
| aegis -- aegis<br>aegis -- aegis-web | aegis 4.24 and aegis-web 4.24 allow local users to overwrite arbitrary files via a symlink attack on (a) /tmp/#####, (b) /tmp/#####.intro, (c) /tmp/aegis.#####.ae, (d) /tmp/aegis.#####, (e) /tmp/aegis.#####.1, (f) /tmp/aegis.#####.2, (g) /tmp/aegis.#####.log, and (h) /tmp/aegis.#####.out temporary files, related to the (1) bng_dvlpd.sh, (2) bng_rvwd.sh, (3) awt_dvlp.sh, (4) awt_intgrtn.sh, and (5) aegis.cgi scripts. | 2008-11-05 | 6. |
| alan_woodland -- ogle<br>alan_woodland -- ogle-mmx | ogle 0.9.2 and ogle-mmx 0.9.2 allow local users to overwrite arbitrary files via a symlink attack on (a) /tmp/ogle_audio.#####, (b) /tmp/ogle_cli.#####, (c) /tmp/ogle_ctrl.#####, (d) /tmp/ogle_gui.#####, (e) /tmp/ogle_mpeg_ps.#####, (f) /tmp/ogle_mpeg_vs.#####, (g) /tmp/ogle_nav.#####, and (h) /tmp/ogle_vout.#####, temporary files, related to the (1) ogle_audio_debug, (2) ogle_cli_debug, (3) ogle_ctrl_debug, (4) ogle_gui_debug, (5) ogle_mpeg_ps_debug, (6) ogle_mpeg_vs_debug, (7) ogle_nav_debug, and (8) ogle_vout_debug scripts. | 2008-11-06 | 6. |
| alastair_mckinstry -- ltp-network-test | ltp-network-test 20060918 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/vsftpd.conf, (b) /tmp/udp/2/*, (c) /tmp/tcp/2/*, (d) /tmp/udp/3/*, (e) /tmp/tcp/3/*, (f) /tmp/nfs_fsstress.udp.2.log, (g) /tmp/nfs_fsstress.udp.3.log, (h) /tmp/nfs_fsstress.tcp.2.log, (i) /tmp/nfs_fsstress.tcp.3.log, and (j) /tmp/nfs_fsstress.sardata temporary files, related to the (1) ftp_setup_vsftp_conf and (2) nfs_fsstress.sh scripts. | 2008-11-06 | 6. |
| alejandro_garrido_mota -- gdrae | gdrae in gdrae 0.1 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/gdrae/palabra temporary file. | 2008-11-05 | 6. |
| amiga -- aview | asciiview in aview 1.3.0 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/aview#####.pgm temporary file. | 2008-11-05 | 6. |

Back to top

## Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVS Sco |
|---|---|---|---|
| apertium -- apertium | apertium 3.0.7 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/#####.lex.cc, (b) /tmp/#####.deformat.l, (c) /tmp/#####.reformat.l, (d) /tmp/#####docxorig, (e) /tmp/#####docxsalida.zip, (f) /tmp/#####xlsxembed, (g) /tmp/#####xlsxorig, and (h) /tmp/#####xslxsalida.zip temporary files, related to the (1) apertium-gen-deformat, (2) apertium-gen-reformat, and (3) apertium scripts. | 2008-11-05 | 6. |
| aptoncd -- aptoncd | xmlfile.py in aptoncd 0.1 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/aptoncd temporary file. | 2008-11-05 | 6. |
| arb_project -- arb-common | arb-common 0.0 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/arb_fdnaml_*, (b) /tmp/arb_pids_*, (c) /tmp/arbdsmz.html, and (d) /tmp/arbdsmz.htm temporary files, related to the (1) arb_fastdnaml and (2) dszmconnect.pl scripts. | 2008-11-05 | 6. |
| audiolink -- audiolink | audiolink in audiolink 0.05 allows local users to overwrite arbitrary files via a symlink attack on the (1) /tmp/audiolink.db.tmp and (2) /tmp/audiolink.tb.tmp temporary files. | 2008-11-05 | 6. |
| bitmover -- lmbench | The (1) rccs and (2) STUFF scripts in lmbench 3.0-a7 allow local users to overwrite arbitrary files via a symlink attack on a /tmp/sdiff.##### temporary file. | 2008-11-06 | 6. |
| cadsoft -- vdr | vdrleaktest in vdr 1.6.0 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/memleaktest.log temporary file. | 2008-11-06 | 6. |
| cce-interact -- interact | SQL injection vulnerability in spaces/emailuser.php in Interact 2.4.1 allows remote attackers to execute arbitrary SQL commands via the email_user_key parameter. | 2008-11-03 | 6. |

Back to top

| Medium Vulnerabilities | | | |
|---|---|---|---|
| **Primary<br>Vendor -- Product** | **Description** | **Published** | **CV<br>Sco** |
| cce-interact -- interact | Cross-site request forgery (CSRF) vulnerability in Interact 2.4.1 allows remote attackers to create super administrator accounts as super administrators. | 2008-11-03 | 6. |
| cdcontrol -- cdcontrol | writtercontrol in cdcontrol 1.90 allows local users to overwrite arbitrary files via a symlink attack on /tmp/v-recorder*-out temporary files. | 2008-11-05 | 6. |
| compact_cms -- compact_cms | Cross-site request forgery (CSRF) vulnerability in CompactCMS 1.1 and earlier allows remote attackers to perform unauthorized actions as legitimate users via unspecified vectors. | 2008-11-03 | 4. |
| debian -- dpkg-cross | ** DISPUTED ** gccross in dpkg-cross 2.3.0 allows local users to overwrite arbitrary files via a symlink attack on the tmp/gccross2.log temporary file. NOTE: the vendor disputes this vulnerability, stating that "There is no sense in this bug - the script ... is called under specific cross-building environments within a chroot." | 2008-11-05 | 6. |
| debian -- myspell | i2myspell in myspell 3.1 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/i2my#####.1 and (2) /tmp/i2my#####.2 temporary files. | 2008-11-06 | 6. |
| debian -- newsgate | mkmailpost in newsgate 1.6 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/mmp##### temporary file. | 2008-11-06 | 6. |
| dovecot -- dovecot | The message parsing feature in Dovecot 1.1.4 and 1.1.5, when using the FETCH ENVELOPE command in the IMAP client, allows remote attackers to cause a denial of service (persistent crash) via an email with a malformed From address, which triggers an assertion error, aka "invalid message address parsing bug." | 2008-11-03 | 4. |
| emacs -- emacs-jabber | emacs-jabber in emacs-jabber 0.7.91 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/*.log temporary file. | 2008-11-05 | 6. |
| firehol -- firehol | ** DISPUTED ** firehol in firehol 1.256 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/.firehol-tmp-#####-*-* and (2) /tmp/firehol.conf temporary files. NOTE: the vendor disputes this vulnerability, stating that an attack "would require an attacker to create | 2008-11-05 | 6. |

| Medium Vulnerabilities | | | |
|---|---|---|---|
| Primary<br>Vendor -- Product | Description | Published | CV<br>Sco |
| | 1073741824*PID-RANGE symlinks." | | |
| firewallbuilder -- fwbuilder | fwb_install in fwbuilder 2.1.19 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/ssh-agent.##### temporary file. | 2008-11-05 | 6. |
| firmchannel -- digital_signage | Cross-site scripting (XSS) vulnerability in the account module in firmCHANNEL Digital Signage 3.24, and possibly earlier versions, allows remote attackers to inject arbitrary web script or HTML via the action parameter to index.php. | 2008-11-05 | 4. |
| freedesktop -- scratchbox2 | scratchbox2 1.99.0.24 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/dpkg.#####.tmp, (b) /tmp/missing_deps.#####, and (c) /tmp/sb2-pkg-chk.$tstamp.##### temporary files, related to the (1) dpkg-checkbuilddeps and (2) sb2-check-pkg-mappings scripts. | 2008-11-06 | 6. |
| freevo -- freevo | freevo.real in freevo 1.8.1 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/*-#####.pid, (2) /tmp/freevo-gdb, (3) /tmp/freevo-gdb.sh, and (4) /tmp/*.stats temporary files. NOTE: this issue is only a vulnerability when a verbose debug mode is activated by modifying source code. | 2008-11-05 | 6. |
| fumitoshi_ukai -- fml | mead.pl in fml 4.0.3 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/debugbuf temporary file. | 2008-11-05 | 6. |
| gccxml -- gccxml | find_flags in gccxml 0.9.0 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/*.cxx temporary file. | 2008-11-05 | 6. |
| georges_khaznadar -- wims | wims 3.62 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/env#####, (b) /tmp/sed#####, and (c) /tmp/referer-home.log temporary files, related to the (1) coqweb and (2) account.sh scripts. | 2008-11-06 | 6. |
| gert_doering -- mgetty | faxspool in mgetty 1.1.36 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/faxsp.##### temporary file. | 2008-11-05 | 6. |
| gplhost -- dtc-common | dtc 0.29.6 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/awstats.log, (b) | 2008-11-05 | 6. |

Back to top

| Medium Vulnerabilities | | | |
|---|---|---|---|
| Primary<br>Vendor -- Product | Description | Published | CV<br>Sco |
| | /tmp/spam.log.#####, and (c) /tmp/spam_err.log temporary files, related to the (1) accesslog.php and (2) sa-wrapper scripts. | | |
| gpsdrive -- gpsdrive-scripts | geo-code in gpsdrive-scripts 2.10~pre4 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/geo.google, (2) /tmp/geo.yahoo, (3) /tmp/geo.coords, and (4) /tmp/geo#####.coords temporary files. | 2008-11-05 | 6. |
| guus_sliepen -- dhis-server | dhis-dummy-log-engine in dhis-server 5.3 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/dhis-dummy-log-engine.log temporary file. | 2008-11-05 | 6. |
| hp -- system_management_homepage | Unspecified vulnerability in HP System Management Homepage (SMH) 2.2.6 and earlier on HP-UX B.11.11 and B.11.23, and SMH 2.2.6 and 2.2.8 and earlier on HP-UX B.11.23 and B.11.31, allows local users to gain "unauthorized access" via unknown vectors, possibly related to temporary file permissions. | 2008-11-04 | 6. |
| iglues -- bulmages-servers | bulmages-servers 0.11.1 allows local users to overwrite arbitrary files via a symlink attack on the (a) /tmp/error.txt, (b) /tmp/errores.txt, and possibly other temporary files, related to the (1) creabulmafact, (2) creabulmacont, and possibly (3) actualizabulmacont, (4) installbulmages-db, and (5) actualizabulmafact scripts. | 2008-11-05 | 6. |
| impose+ -- impose+ | impose in impose+ 0.2 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/*-tmp.ps and (2) /tmp/bboxx-* temporary files. | 2008-11-05 | 6. |
| krzysztof_kozlowski -- konwert | filters/any-UTF8 in konwert 1.8 allows local users to delete arbitrary files via a symlink attack on a /tmp/any-##### temporary file. | 2008-11-06 | 6. |
| lars_bahner -- xcal | pscal in xcal 4.1 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/pscal##### temporary file. | 2008-11-06 | 6. |
| linux -- kernel | arch/i386/kernel/sysenter.c in the Virtual Dynamic Shared Objects (vDSO) implementation in the Linux kernel before 2.6.21 does not properly check boundaries, which allows local users to gain privileges or cause a denial of service via unspecified vectors, related to the install_special_mapping, | 2008-11-05 | 4. |

**Medium Vulnerabilities**

| Primary Vendor -- Product | Description | Published | CV Sco |
|---|---|---|---|
| | syscall, and syscall32_nopage functions. | | |
| linuxtrade -- linuxtrade | linuxtrade 3.65 allows local users to overwrite arbitrary files via a symlink attack on the (a) /tmp/bwk, (b) /tmp/zzz, and (c) /tmp/ggg temporary files, related to the (1) linuxtrade.bwkvol, (2) linuxtrade.wn, and (3) moneyam.helper scripts. | 2008-11-06 | 6. |
| logz -- logz | Cross-site scripting (XSS) vulnerability in fichiers/add_url.php in Logz CMS 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the art parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | 2008-11-03 | 4. |
| logz -- logz | SQL injection vulnerability in fichiers/add_url.php in Logz podcast CMS 1.3.1, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the art parameter. | 2008-11-03 | 6. |
| lokicms -- lokicms | Directory traversal vulnerability in admin.php in LokiCMS 0.3.3 and earlier allows remote attackers to delete arbitrary files via a .. (dot dot) in the delete parameter. | 2008-11-03 | 5. |
| lustre -- lustre-tests | runiozone in lustre 1.6.5 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/iozone.log temporary file. | 2008-11-06 | 6. |
| mafft -- mafft | mafft-homologs in mafft 6.240 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/_vf#?????, (2) /tmp/_if#?????, (3) /tmp/_pf#?????, (4) /tmp/_af#?????, (5) /tmp/_rid#?????, (6) /tmp/_res#?????, (7) /tmp/_q#?????, and (8) /tmp/_bf#????? temporary files. | 2008-11-06 | 6. |
| manoj_srivastava -- dist | dist 3.5 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/cil#####, (b) /tmp/pdo#####, and (c) /tmp/pdn##### temporary files, related to the (1) patcil and (2) patdiff scripts. | 2008-11-05 | 6. |
| mybb -- mybb | Cross-site scripting (XSS) vulnerability in the redirect function in functions.php in MyBB (aka MyBulletinBoard) 1.4.2 allows remote attackers to inject arbitrary web script or HTML via the url parameter in a removesubscriptions action to moderation.php, related to use of the ajax option to request a JavaScript redirect. NOTE: this can be leveraged to execute PHP code and bypass cross-site request forgery (CSRF) protection. | 2008-11-04 | 4. |

Back to top

## Medium Vulnerabilities

| Primary<br>Vendor -- Product | Description | Published | CV<br>Sco |
|---|---|---|---|
| mybb -- mybb | MyBB (aka MyBulletinBoard) 1.4.2 uses insufficient randomness to compose filenames of uploaded files used as attachments, which makes it easier for remote attackers to read these files by guessing filenames. | 2008-11-04 | 5. |
| mybb -- mybb | MyBB (aka MyBulletinBoard) 1.4.2 does not properly handle an uploaded file with a nonstandard file type that contains HTML sequences, which allows remote attackers to cause that file to be processed as HTML by Internet Explorer's content inspection, aka "Incomplete protection against MIME-sniffing." NOTE: this could be leveraged for XSS and other attacks. | 2008-11-04 | 5. |
| net-snmp -- net-snmp | Integer overflow in the netsnmp_create_subtree_cache function in agent/snmp_agent.c in net-snmp 5.4 before 5.4.2.1, 5.3 before 5.3.2.3, and 5.2 before 5.2.5.1 allows remote attackers to cause a denial of service (crash) via a crafted SNMP GETBULK request, which triggers a heap-based buffer overflow, related to the number of responses or repeats. | 2008-10-31 | 5. |
| netmrg -- netmrg | rrdedit in netmrg 0.20 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/*.xml and (2) /tmp/*.backup temporary files. | 2008-11-06 | 6. |
| netrisk -- netrisk | Cross-site scripting (XSS) vulnerability in index.php in NetRisk 2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the error parameter. | 2008-11-03 | 4. |
| nostatic -- digitaldj | fest.pl in digitaldj 0.7.5 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/ddj_fest.tmp temporary file. | 2008-11-05 | 6. |
| openswan -- linux-patch-openswan | linux-patch-openswan 2.4.12 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/snap##### and (b) /tmp/nightly##### temporary files, related to the (1) maysnap and (2) maytest scripts. | 2008-11-06 | 6. |
| planetluc -- signme | Cross-site scripting (XSS) vulnerability in signme.inc.php in Planetluc SignMe 1.5 before 1.55 allows remote attackers to inject arbitrary web script or HTML via the hash parameter. NOTE: some of these details are obtained from third party information. | 2008-11-03 | 4. |
| planetluc -- mygallery | Cross-site scripting (XSS) vulnerability in gallery.inc.php in Planetluc MyGallery 1.7.2 and earlier, and possibly other versions before 1.8.1, allows remote attackers to inject arbitrary web script or HTML via the mghash parameter. NOTE: some of these details are obtained from third party information. | 2008-11-03 | 4. |

Back to top

| Medium Vulnerabilities | | | |
|---|---|---|---|
| **Primary<br>Vendor -- Product** | **Description** | **Published** | **CV<br>Sco** |
| planetluc -- rateme | Cross-site scripting (XSS) vulnerability in planetluc RateMe 1.3.3 allows remote attackers to inject arbitrary web script or HTML via the rate parameter in a submit rate action. | 2008-11-03 | 4. |
| planetluc -- rateme | Cross-site request forgery (CSRF) vulnerability in Planetluc RateMe 1.3.3 allows remote attackers to perform unauthorized actions as other users via unspecified vectors. | 2008-11-03 | 6. |
| postfix -- postfix | ** DISPUTED ** postfix_groups.pl in Postfix 2.5.2 allows local users to overwrite arbitrary files via a symlink attack on the (1) /tmp/postfix_groups.stdout, (2) /tmp/postfix_groups.stderr, and (3) /tmp/postfix_groups.message temporary files. NOTE: the vendor disputes this vulnerability, stating "This is not a real issue ... users would have to edit a script under /usr/lib to enable it." | 2008-11-06 | 6. |
| radiance -- radiance | radiance 3R9+20080530 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/opt.fmt, (b) /tmp/out#####.fmt, (c) /tmp/tf#####.dat, (d) /tmp/gsf#####, (e) /tmp/sc#####.sh, (f) /tmp/il#####.pic, (g) /tmp/tl#####.pic, (h) /tmp/ds#####.pic, (i) /tmp/tfa#####, and (j) /tmp/sed##### temporary files, related to the (1) optics2rad, (2) pdelta, (3) dayfact, and (4) raddepend scripts. | 2008-11-06 | 6. |
| remi_vanicat -- realtimebattle | perl.robot in realtimebattle 1.0.8 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/perl.robot.log temporary file. | 2008-11-06 | 6. |
| rkhunter -- rkhunter | rkhunter in rkhunter 1.3.2 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/rkhunter-debug temporary file. NOTE: this is probably a different vulnerability than CVE-2005-1270. | 2008-11-06 | 6. |
| savonet -- liguidsoap | liguidsoap.py in liguidsoap 0.3.8.1+2 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/liguidsoap.liq, (2) /tmp/lig.#####.log, and (3) /tmp/emission.ogg temporary files. | 2008-11-06 | 6. |
| scilab -- scilab-bin | scilab-bin 4.1.2 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/SciLink#####1, (b) /tmp/SciLink#####2, (c) /tmp/SciLink#####3, (d) /tmp/*.#####, (e) /tmp/*.#####.res, (f) /tmp/*.#####.err, and (g) /tmp/*.#####.diff temporary files, related to the (1) scilink, (2) scidoc, and (3) scidem scripts. | 2008-11-06 | 6. |

Back to top

| Medium Vulnerabilities | | | |
|---|---|---|---|
| Primary Vendor -- Product | Description | Published | CV Sco |
| shrubbery -- rancid | getipacctg in rancid 2.3.2~a8 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/ipacct.#####.prefixes, (2) /tmp/ipacct.#####.sorted, (3) /tmp/ipacct.#####.pl, and (4) /tmp/ipacct.##### temporary files. | 2008-11-06 | 6. |
| simple_php_scripts -- blog | Cross-site scripting (XSS) vulnerability in complete.php in Simple PHP Scripts blog 0.3 allows remote attackers to inject arbitrary web script or HTML via the id parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | 2008-10-31 | 4. |
| sonicwall -- sonicos | Cross-site scripting (XSS) vulnerability in SonicWALL SonicOS Enhanced before 4.0.1.1, as used in SonicWALL Pro 2040 and TZ 180 and 190, allows remote attackers to inject arbitrary web script or HTML into arbitrary web sites via a URL to a site that is blocked based on content filtering, which is not properly handled in the CFS block page, aka "universal website hijacking." | 2008-11-04 | 4. |
| steve_robbins -- mgt | mailgo in mgt 2.31 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/mailgo##### temporary file. | 2008-11-06 | 6. |
| sun -- blade_t6300_server<br>sun -- blade_t6320_server<br>sun -- fire_enterprise_server_t1000<br>sun -- fire_enterprise_server_t2000<br>sun -- netra_cp3060_server<br>sun -- netra_t2000_server<br>sun -- netra_t5220_server<br>sun -- sparc_enterprise_server_t1000<br>sun -- sparc_enterprise_server_t2000<br>sun -- sparc_enterprise_server_t5120<br>sun -- sparc_enterprise_server_t5140<br>sun -- sparc_enterprise_server_t5220 | The SPARC hypervisor in Sun System Firmware 6.6.3 through 6.6.5 and 7.1.3 through 7.1.3.e on UltraSPARC T1, T2, and T2+ processors allows logical domain users to access memory in other logical domains via unknown vectors. | 2008-11-07 | 4. |

Back to top

**Medium Vulnerabilities**

| Primary Vendor -- Product | Description | Published | CV Sco |
|---|---|---|---|
| sun -- sparc_enterprise_server_t5240 | | | |
| tivano -- cdrw-taper | amlabel-cdrw in cdrw-taper 0.4 might allow local users to overwrite arbitrary files via a symlink attack involving a /tmp/amlabel-cdrw.##### temporary directory. | 2008-11-05 | 6. |
| tribiq -- tribiq_cms | Directory traversal vulnerability in templates/mytribiqsite/tribal-GPL-1066/includes/header.inc.php in Tribiq CMS 5.0.10a, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the template_path parameter. | 2008-11-03 | 5. |
| typosphere -- typo | Cross-site scripting (XSS) vulnerability in the leave comment (feedback) feature in Typo 5.1.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the (1) comment[author] (Name) and (2) comment[url] (Website) parameters. | 2008-11-03 | 4. |
| typosphere -- typo | SQL injection vulnerability in the "Manage pages" feature (admin/pages) in Typo 5.1.3 and earlier allows remote authenticated users with "blog publisher" rights to execute arbitrary SQL commands via the search[published_at] parameter. | 2008-11-03 | 6. |
| typosphere -- typo | Typo 5.1.3 and earlier uses a hard-coded salt for calculating password hashes, which makes it easier for attackers to guess passwords via a brute force attack. | 2008-11-03 | 5. |
| xastir -- xastir | xastir 1.9.2 allows local users to overwrite arbitrary files via a symlink attack on the (a) /tmp/ldconfig.tmp, (b) /tmp/ldconf.tmp, and (c) /tmp/ld.so.conf temporary files, related to the (1) get-maptools.sh and (2) get_shapelib.sh scripts. | 2008-11-06 | 6. |
| xenman -- convirt | convirt 0.8.2 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/set_output temporary file, related to the (1) _template_/provision.sh, (2) Linux_CD_Install/provision.sh, (3) Fedora_PV_Install/provision.sh, (4) CentOS_PV_Install/provision.sh, (5) common/provision.sh, (6) example/provision.sh, and (7) Windows_CD_Install/provision.sh scripts in image_store/. | 2008-11-05 | 6. |
| zak_b_elep -- rccp | delqueueask in rccp 0.9 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/cccp_tmp.txt temporary file. | 2008-11-06 | 6. |

Back to top

## Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| crossfire -- crossfire | maps/Info/combine.pl in CrossFire crossfire-maps 1.11.0 allows local users to overwrite arbitrary files via a symlink attack on a temporary file. | 2008-11-03 | 3.3 | CVE-2008-4908<br>BID |
| tribiq -- tribiq_cms | Cross-site scripting (XSS) vulnerability in templates/mytribiqsite/tribal-GPL-1066/includes/header.inc.php in Tribiq CMS 5.0.10a, when register_globals is enabled, allows remote attackers to inject arbitrary web script or HTML via the template_path parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | 2008-11-03 | 2.6 | CVE-2008-4893<br>BID<br>SECUNIA |
| xen -- xen | qemu-dm.debug in Xen 3.2.1 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/args temporary file. | 2008-11-07 | 3.3 | CVE-2008-4993<br>CONFIRM<br>CONFIRM<br>MLIST<br>CONFIRM<br>CONFIRM |

Back to top

| Low Vulnerabilities | | | | |
|---|---|---|---|---|
| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
| Back to top | | | | |