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
Arif Supriyanto -- auraCMS	Multiple cross-site scripting (XSS) vulnerabilities in Arif Supriyanto auraCMS 1.62 allow remote attackers to inject arbitrary web script or HTML via (1) the judul_artikel parameter in teman.php and (2) the title of an article sent to admin, which is displayed when unauthenticated users visit index.php.	unknown 2006-07-12	7.0	CVE-2006-3558 BUGTRAQ OTHER-REF BID
Arif Supriyanto -- auraCMS	Multiple SQL injection vulnerabilities in Arif Supriyanto auraCMS 1.62 allow remote attackers to execute arbitrary SQL commands and delete all shoutbox messages via the (1) name and (2) pesan parameters.	unknown 2006-07-12	7.0	CVE-2006-3559 BUGTRAQ OTHER-REF BID
AstroDog Press -- Some Chess	Multiple SQL injection vulnerabilities in AstroDog Press Some Chess 1.5-RC2 and earlier allow remote attackers to execute arbitrary SQL commands via unspecified vectors, possibly including the gameID parameter in board.php.	unknown 2006-07-10	7.0	CVE-2006-3485 OTHER-REF BID FRSIRT OSVDB SECUNIA XF
Belchior Foundry -- vCard	Multiple SQL injection vulnerabilities in Belchior Foundry vCard PRO allow remote attackers to execute arbitrary SQL commands via the (1) cat_id parameter to (a) gbrowse.php, (2) card_id parameter to (b) rating.php and (c) create.php, and the (3) event_id parameter to (d) search.php.	unknown 2006-07-10	7.0	CVE-2006-3474 BUGTRAQ BID XF
Blue Dojo -- Graffiti Forums	SQL injection vulnerability in topics.php in Blue Dojo Graffiti Forums 1.0 allows remote attackers to execute arbitrary SQL commands via the f parameter.	unknown 2006-07-12	7.0	CVE-2006-3560 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
BosDev -- BosClassifieds Classified Ads	Multiple PHP remote file inclusion vulnerabilities in BosClassifieds Classified Ads allow remote attackers to execute arbitrary PHP code via a URL in the insPath parameter to (1) index.php, (2) recent.php, (3) account.php, (4) classified.php, or (5) search.php.	unknown 2006-07-11	7.0	CVE-2006-3527 OTHER-REF BID SECTRACK
Christophe Thibault -- Kaillera	Stack-based buffer overflow in Kaillera Server 0.86 and earlier allows remote attackers to execute arbitrary code via a long nickname.	unknown 2006-07-10	7.0	CVE-2006-3491 FULLDISC OTHER-REF BID FRSIRT SECUNIA
Dell -- Openmanage CD	The Dell Openmanage CD launches X11 and SSH daemons that do not require authentication, which allows remote attackers to gain privileges.	unknown 2006-07-10	7.0	CVE-2006-3470 BUGTRAQ CERT-VN

				XF
Drupal -- form_mail module	CRLF injection vulnerability in form_mail Drupal Module before 1.8.2.2 allows remote attackers to inject e-mail headers, which facilitates sending spam messages, a different issue than CVE-2006-1225.	unknown 2006-07-10	7.0	CVE-2006-3473 OTHER-REF FRSIRT SECUNIA XF
eBay -- Enhanced Picture Services	Buffer overflow in eBay Enhanced Picture Services (aka EPUImageControl Class) in EUPWALcontrol.dll before 1.0.3.48, as used in Sell Your Item (SYI), Setup & Test eBay Enhanced Picture Services, Picture Manager Enhanced Uploader, and CARad.com Add Vehicle, allows remote attackers to execute arbitrary code via a crafted HTML document.	unknown 2006-07-07	7.0	CVE-2006-1176 OTHER-REF CERT-VN FRSIRT SECTRACK SECUNIA XF
ExtCalendar -- ExtCalendar	PHP remote file inclusion vulnerability in extcalendar.php in Mohamed Moujami ExtCalendar 2.0 allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	unknown 2006-07-12	7.0	CVE-2006-3556 BUGTRAQ ECHO BID
Fantastic -- Guestbook	Multiple cross-site scripting (XSS) vulnerabilities in guestbook.php in Fantastic Guestbook 2.0.1, and possibly earlier versions, allow remote attackers to inject arbitrary web script or HTML via the (1) first_name, (2) last_name, or (3) nickname parameters.	2006-07-11 2006-07-12	7.0	CVE-2006-3568 OTHER-REF BID FRSIRT SECUNIA
free QBoard -- free QBoard	Multiple PHP remote file inclusion vulnerabilities in free QBoard 1.1 allow remote attackers to execute arbitrary PHP code via a URL in the qb_path parameter to (1) index.php, (2) about.php, (3) contact.php, (4) delete.php, (5) faq.php, (6) features.php or (7) history.php, a different set of vectors than CVE-2006-2998.	unknown 2006-07-10	7.0	CVE-2006-3475 BUGTRAQ BID SECTRACK XF
FreeHost -- FreeHost	Multiple SQL injection vulnerabilities in FreeHost allow remote attackers to execute arbitrary SQL commands via (1) readme parameter to FreeHost/misc.php or (2) index parameter to FreeHost/news.php.	unknown 2006-07-11	7.0	CVE-2006-3516 BUGTRAQ
Fujitsu -- ServerView	Cross-site scripting (XSS) vulnerability in Fujitsu ServerView 2.50 up to 3.60L98 and 4.10L11 up to 4.11L81 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2006-07-13	7.0	CVE-2006-3579 JVN JVN FUJITSU SECUNIA
Hitachi -- Groupmax Collaboration Web Client Hitachi -- Groupmax Collaboration Portal Hitachi -- Cosminexus Collaboration Portal	Multiple cross-site scripting (XSS) vulnerabilities in Hitachi Groupmax Collaboration Portal and Web Client before 07-20-/D, and uCosminexus Collaboration Portal and Forum/File Sharing before 06-20-/C, allow remote attackers to "execute malicious scripts" via unknown vectors (aka HS06-014-01).	unknown 2006-07-13	7.0	CVE-2006-3574 HITACHI HITACHI BID FRSIRT SECUNIA
HiveMail -- HiveMail	SQL injection vulnerability in search.results.php in HiveMail 3.1 and earlier allows remote attackers to execute arbitrary SQL commands via the fields[] parameter.	unknown 2006-07-12	7.0	CVE-2006-3565 OTHER-REF SECUNIA
IBM -- Network Appliance Data ONTAP	Unspecified vulnerability in IBM Data ONTAP 7.1 and 7.1.0.1, when used with IBM N series Filers, causes it to "expose commands" to local users via unknown vectors, probably related to incorrect capabilities with the audit role. NOTE: it is not clear whether IBM's use of the "expose" term means that previously executed commands can be viewed, or if the user obtains access to commands that are otherwise restricted.	unknown 2006-07-12	7.0	CVE-2006-3569 OTHER-REF FRSIRT SECUNIA XF
Invision Power Services -- Invision Power Board	Multiple SQL injection vulnerabilities in Invision Power Board (IPB) 1.x and 2.x allow remote attackers to execute arbitrary SQL commands via the (1) idcat and (2) code parameters in a ketqua action in index.php; the id parameter in a (3) Attach and (4) ref action in index.php; the CODE parameter in a (5) Profile, (6) Login, and (7) Help action in index.php; and the (8) member_id parameter in coins_list.php.	unknown 2006-07-12	7.0	CVE-2006-3543 BUGTRAQ BID
Joomla -- Joomla	Multiple SQL injection vulnerabilities in Joomla! before 1.0.10 allow remote attackers to execute arbitrary SQL commands via unspecified parameters involving the (1) "Remember Me" function, (2) "Related	unknown 2006-07-10	7.0	CVE-2006-3481 OTHER-REF OTHER-REF

	Items" module, and the (3) "Weblinks submission".			BID FRSIRT SECUNIA
MamboXChange -- SimpleBoard	Multiple PHP remote file inclusion vulnerabilities in Simpleboard Mambo module 1.1.0 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the sbp parameter to (1) image_upload.php and (2) file_upload.php.	unknown 2006-07-11	7.0	CVE-2006-3528 OTHER-REF BID FRSIRT SECUNIA
Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Windows XP	Heap-based buffer overflow in the Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to execute arbitrary code via crafted first-class Mailslot messages that triggers memory corruption and bypasses size restrictions on second-class Mailslot messages.	unknown 2006-07-11	7.0	CVE-2006-1314 OTHER-REF MS BUGTRAQ CERT-VN XF
Microsoft -- DHCP Client Service	Buffer overflow in the DHCP Client service for Microsoft Windows 2000 SP4, Windows XP SP1 and SP2, and Server 2003 up to SP1 allows remote attackers to execute arbitrary code via a crafted DHCP response.	2005-12-26 2006-07-11	7.0	CVE-2006-2372 BUGTRAQ OTHER-REF MS BID FRSIRT SECUNIA
Microsoft -- Excel	Buffer overflow in certain Asian language versions of Microsoft Excel might allow user-complicit attackers to execute arbitrary code via a crafted spreadsheet that triggers the overflow when the user attempts to repair the document or selects the "Style" option, as demonstrated by nanika.xls. NOTE: Microsoft has confirmed to CVE via e-mail that this is different than the other Excel vulnerabilities announced before 20060707, including CVE-2006-3059 and CVE-2006-3086.	unknown 2006-07-07	7.0	CVE-2006-3431 BUGTRAQ BUGTRAQ BID FRSIRT SECUNIA SECTRACK
MKPortal -- MKPortal	Directory traversal vulnerability in index.php in MKPortal 1.0.1 Final allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the language cookie, as demonstrated by using a gl_session cookie to inject PHP sequences into the error.log file, which is then included by index.php with malicious commands accessible by the ind parameter.	unknown 2006-07-12	7.0	CVE-2006-3554 BUGTRAQ OTHER-REF FRSIRT SECTRACK SECUNIA
myiosoft.com -- AjaxPortal	SQL injection vulnerability in the loginADP function in ajaxp.php in AjaxPortal 3.0 allows remote attackers to execute arbitrary SQL commands and bypass authentication via the (1) username or (2) password parameters.	unknown 2006-07-11	7.0	CVE-2006-3515 BUGTRAQ OTHER-REF BID FRSIRT
MyPHP CMS -- MyPHP CMS	PHP remote file inclusion vulnerability in styles/default/global_header.php in MyPHP CMS 0.3 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the domain parameter.	unknown 2006-07-10	7.0	CVE-2006-3478 OTHER-REF BID FRSIRT XF
Papoo -- Papoo	SQL injection vulnerability in forumthread.php in Papoo 3 RC3 and earlier allows remote attackers to execute arbitrary SQL commands via the msgid parameter.	2006-07-07 2006-07-12	7.0	CVE-2006-3572 BUGTRAQ Milw0rm BID FRSIRT SECTRACK SECUNIA XF
PlaNet Concept -- planetNews	PlaNet Concept planetNews allows remote attackers to bypass authentication and execute arbitrary code via a direct request to news/admin/planetnews.php.	2006-06-26 2006-07-12	10.0	CVE-2006-3553 BUGTRAQ SECTRACK
Plume CMS -- Plume CMS	PHP remote file inclusion vulnerabilities in plume cms 1.0.4 allow remote attackers to execute arbitrary PHP code via a URL in the _PX_config[manager_path] parameter to (1) index.php, (2) rss.php, or (3) search.php, a different set of vectors and versions than CVE-2006-2645 and CVE-2006-0725.	unknown 2006-07-12	7.0	CVE-2006-3562 BUGTRAQ BID SECTRACK XF

Randshop -- Randshop	PHP remote file inclusion vulnerability in index.php in Randshop before 1.2 allows remote attackers to execute arbitrary PHP code via the dateiPfad parameter, a different vector than CVE-2006-3375.	2006-07-06 2006-07-12	7.0	CVE-2006-3537 BUGTRAQ BID FRSIRT XF
rwscripts.com -- RW::Download	PHP remote file inclusion vulnerability in stats.php in RW::Download, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the root_path parameter.	unknown 2006-07-11	7.0	CVE-2006-3517 BUGTRAQ BID
Simian Systems Inc -- SiteForge Collaborative Development Platform	Multiple cross-site scripting (XSS) vulnerabilities in index/siteforge-bugs-action/proj.siteforge in SiteForge Collaborative Development Platform 1.0.4 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) _status, (2) _extra1, (3) _extra2, or (4) _extra3 parameters.	unknown 2006-07-11	7.0	CVE-2006-3521 OTHER-REF XF
Vastal I-Tech -- Buddy Zone	Multiple SQL injection vulnerabilities in Buddy Zone 1.0.1 allow remote attackers to execute arbitrary SQL commands via the (1) cat_id parameter to (a) view_classifieds.php; (2) id parameter in (b) view_ad.php; (3) event_id parameter in (c) view_event.php, (d) delete_event.php, and (e) edit_event.php; and (4) group_id in (f) view_group.php.	unknown 2006-07-10	7.0	CVE-2006-3494 BUGTRAQ FRSIRT OSVDB OSVDB OSVDB OSVDB OSVDB OSVDB OSVDB SECUNIA
webvizyon.net -- Webvizyon Portal	SQL injection vulnerability in SayfalaAltList.asp in Webvizyon Portal 2006 allows remote attackers to execute arbitrary SQL commands via the ID parameter.	unknown 2006-07-11	7.0	CVE-2006-3518 BUGTRAQ BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Adobe -- Acrobat Adobe -- Acrobat Reader	Adobe Reader and Acrobat 6.0.4 and earlier, on Mac OSX, has insecure file and directory permissions, which allows local users to gain privileges by overwriting program files.	unknown 2006-07-12	4.9	CVE-2006-3452 ADOBE BID FRSIRT SECUNIA
ASP Stats Generator -- ASP Stats Generator	SQL injection vulnerability in pages.asp in ASP Stats Generator before 2.1.2 allows remote attackers to execute arbitrary SQL commands via the order parameter.	unknown 2006-07-13	4.7	CVE-2006-3580 OTHER-REF OTHER-REF SECTRACK
BeatificFaith -- Eprayer	Multiple cross-site scripting (XSS) vulnerabilities in demo.php in BeatificFaith Eprayer Alpha allow remote attackers to inject arbitrary web script or HTML via the SRC attribute of a SCRIPT element in the (1) "Your name" field and (2) "Enter Prayer Request here" field.	unknown 2006-07-12	4.7	CVE-2006-3538 BUGTRAQ OTHER-REF OTHER-REF BID XF
EJ3 -- TOPo	Direct static code injection vulnerability in code/class_db_text.php in EJ3 TOPo 2.2.178 and earlier allows remote attackers to execute arbitrary PHP code via parameters such as (1) descripcion and (2) pais, which are stored directly in a PHP script. NOTE: the provenance of this information is unknown; the details are obtained solely from third party reports.	unknown 2006-07-12	4.7	CVE-2006-3536 BID FRSIRT
Fujitsu -- ServerView	Directory traversal vulnerability in Fujitsu ServerView 2.50 up to 3.60L98 and 4.10L11 up to 4.11L81 allows remote attackers to read arbitrary files via unspecified vectors.	unknown 2006-07-13	4.7	CVE-2006-3578 OTHER-REF OTHER-REF OTHER-REF SECUNIA

Garry Glendown -- Shopping Cart	Multiple cross-site scripting (XSS) vulnerabilities in Garry Glendown Shopping Cart 0.9 allow remote attackers to inject arbitrary web script or HTML via the (1) shop name field in (a) editshop.php, (b) edititem.php, and (c) index.php; and via the (2) item field in editshop.php and edititem.php.	unknown 2006-07-12	4.7	CVE-2006-3542 BUGTRAQ BID
Invision Power Services -- Invision Board	Multiple SQL injection vulnerabilities in Invision Power Board (IPB) 1.3 Final allow remote attackers to execute arbitrary SQL commands via the CODE parameter in a (1) Stats, (2) Mail, and (3) Reg action in index.php.	unknown 2006-07-12	4.7	CVE-2006-3544 BUGTRAQ BID
Ipswitch -- Ipswitch Collaboration Suite Ipswitch -- Ipswitch Secure Server	Premium Anti-Spam in Ipswitch IMail Secure Server 2006 and Collaboration Suite 2006 Premium, when using a certain .dat file in the StarEngine /data directory from 20060630 or earlier, does not properly receive and implement bullet signature updates, which allows context-dependent attackers to use the server for spam transmission.	unknown 2006-07-12	4.7	CVE-2006-3552 OTHER-REF OTHER-REF FRSIRT SECTRACK SECTRACK
Joomla -- Joomla	Multiple cross-site scripting (XSS) vulnerabilities in Joomla! before 1.0.10 allow remote attackers to inject arbitrary web script or HTML via unspecified parameters involving the (1) getUserStateFromRequest function, and the (2) SEF and (3) com_messages modules.	unknown 2006-07-10	4.7	CVE-2006-3480 OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Joomla! -- pc_cookbook Mambo -- pc_cookbook	PHP remote file inclusion vulnerability in com_pccookbook/pccookbook.php in the PccookBook Component for Mambo and Joomla 0.3 and possibly up to 1.3.1, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via the mosConfig_absolute_path parameter.	unknown 2006-07-12	5.6	CVE-2006-3530 BUGTRAQ ECHO BID FRSIRT SECUNIA
Kyberna -- ky2help	SQL injection vulnerability in Meine Links (aka My Links) in Kyberna ky2help allows remote authenticated users to execute arbitrary SQL commands via unspecified "textboxes."	2005-10-27 2006-07-12	4.2	CVE-2006-3541 BUGTRAQ OTHER-REF BID
LifeType -- LifeType	SQL injection vulnerability in index.php in LifeType 1.0.5 allows remote attackers to execute arbitrary SQL commands via the Date parameter in a Default op.	unknown 2006-07-13	4.7	CVE-2006-3577 OTHER-REF BID
Linux -- Linux kernel	The suid_dumpable support in Linux kernel 2.6.13 up to versions before 2.6.17.4, and 2.6.16 before 2.6.16.24, allows a local user to cause a denial of service (disk consumption) and possibly gain privileges via the PR_SET_DUMPABLE argument of the prctl function and a program that causes a core dump file to be created in a directory for which the user does not have permissions.	unknown 2006-07-07	4.9	CVE-2006-2451 OTHER-REF REDHAT OTHER-REF OTHER-REF OTHER-REF FRSIRT UBUNTU BID SECUNIA
Microsoft -- Office	Unspecified vulnerability in Microsoft Office 2003 SP1 and SP2, Office XP SP3, Office 2000 SP3, and other products, allows user-complicit attackers to execute arbitrary code via a crafted GIF image that triggers memory corruption when it is parsed.	unknown 2006-07-11	5.6	CVE-2006-0007 MS CERT-VN BID FRSIRT SECUNIA
Microsoft -- IIS	Buffer overflow in Microsoft Internet Information Services (IIS) 5.0, 5.1, and 6.0 allows local and possibly remote attackers to execute arbitrary code via crafted Active Server Pages (ASP).	unknown 2006-07-11	4.2	CVE-2006-0026 MS CERT-VN BID FRSIRT SECTRACK SECUNIA XF
Microsoft -- Office	Unspecified vulnerability in Microsoft Office 2003 SP1 and SP2, Office XP SP3, Office 2000 SP3, and other products, allows user-complicit attackers to execute arbitrary code via an Office file with malformed string that triggers memory corruption related to record lengths, aka "Microsoft Office Parsing Vulnerability," a	unknown 2006-07-11	5.6	CVE-2006-1316 MS CERT-VN FRSIRT SECUNIA

	different vulnerability than CVE-2006-2389.			XF
Microsoft -- Office	Unspecified vulnerability in Microsoft Office 2003 SP1 and SP2, Office XP SP3, Office 2000 SP3, and other products, allows user-complicit attackers to execute arbitrary code via an Office file with a malformed property that triggers memory corruption related to record lengths, aka "Microsoft Office Property Vulnerability," a different vulnerability than CVE-2006-1316.	unknown 2006-07-11	5.6	CVE-2006-2389 MS CERT-VN FRSIRT SECUNIA XF
Microsoft -- Office	Buffer overflow in LsCreateLine function (mso_203) in mso.dll and mso9.dll, as used by Microsoft Word and possibly other products in Microsoft Office 2003, 2002, andd 2000, allows remote user-complicit attackers to cause a denial of service (crash) via a crafted Word DOC or other Office file type. NOTE: this issue was originally reported to allow code execution, but on 20060710 Microsoft stated that code execution is not possible, and the original researcher agrees.	unknown 2006-07-10	5.6	CVE-2006-3493 FULLDISC BID FRSIRT SECTRACK OTHER-REF FULLDISC XF
Milan Mimica -- Sparklet	Format string vulnerability in agl_text.cpp in Milan Mimica Sparklet 0.9.4 and earlier allows remote attackers to execute arbitrary code via format string specifiers in a player nickname.	unknown 2006-07-13	4.7	CVE-2006-3573 OTHER-REF BID
Native Solutions -- The Banner Engine	Multiple cross-site scripting (XSS) vulnerabilities in The Banner Engine (tbe) 4.0 allow remote attackers to execute arbitrary web script or HTML via the (1) text parameter in a search action to (a) top.php, and the (2) adminpass or (3) adminlogin parameter to (b) signup.php.	unknown 2006-07-11	4.7	CVE-2006-3519 BUGTRAQ FRSIRT SECTRACK SECUNIA
PHP-Fusion -- PHP-Fusion	Multiple cross-site scripting (XSS) vulnerabilities in submit.php in PHP-Fusion before 6.01.3 allow remote attackers to inject arbitrary web script or HTML by using edit_profile.php to upload a (1) avatar or (2) forum image attachment that has a .gif or .jpg extension, and begins with a GIF header followed by JavaScript code, which is executed by Internet Explorer.	unknown 2006-07-12	4.7	CVE-2006-3555 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA XF
PHPCredo -- PHCDownload	SQL injection vulnerability in category.php in PHCDownload 1.0.0 Final and 1.0.0 Release Candidate 6 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-07-11	4.7	CVE-2006-3525 OTHER-REF XF
PHPMailList -- PHPMailList	Cross-site scripting (XSS) vulnerability in maillist.php in PHPMailList 1.8.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the email parameter.	2006-06-06 2006-07-10	5.6	CVE-2006-3482 OTHER-REF BID SECTRACK SECUNIA
Pivot -- Pivot	includes/editor/insert_image.php in Pivot 1.30 RC2 and earlier creates the authentication credentials from parameters, which allows remote attackers to obtain privileges and upload arbitrary files via modified (1) pass and (2) session parameters, and (3) pass and (4) userlevel indices of the (a) Pivot_Vars[] or (b) Users[] array parameters.	unknown 2006-07-12	4.7	CVE-2006-3531 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Pivot -- Pivot	PHP file inclusion vulnerability in includes/edit_new.php in Pivot 1.30 RC2 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a FTP URL or full file path in the Paths[extensions_path] parameter.	unknown 2006-07-12	4.7	CVE-2006-3532 BUGTRAQ OTHER-REF BID SECUNIA
Pivot -- Pivot	Multiple cross-site scripting (XSS) vulnerabilities in Pivot 1.30 RC2 and earlier, when register_globals is enabled, allow remote attackers to inject arbitrary web script or HTML via the (1) fg, (2) line1, (3) line2, (4) bg, (5) c1, (6) c2, (7) c3, and (8) c4 parameters in (a) includes/blogroll.php; (9) name and (10) js_name parameters in (b) includes/editor/edit_menu.php; and, even if register_globals is not enabled, the (11) h and (12) w parameters in (c) includes/photo.php.	unknown 2006-07-12	4.7	CVE-2006-3533 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Sabdrimer CMS -- Sabdrimer CMS	PHP remote file inclusion vulnerability in skins/advanced/advanced1.php in Sabdrimer Pro 2.2.4, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the pluginpath[0] parameter.	unknown 2006-07-11	4.7	CVE-2006-3520 OTHER-REF BID FRSIRT

SenseSites -- CommonSense	SQL injection vulnerability in Search.PHP in SenseSites CommonSense CMS 5.0 allows remote attackers to execute arbitrary SQL commands via the Date parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-07-13	4.7	CVE-2006-3576 BID
SIPfoundry -- sipXtapi	Buffer overflow in SIPfoundry sipXtapi released before 20060324 allows remote attackers to execute arbitrary code via a long CSeq field value in an INVITE message.	unknown 2006-07-11	4.7	CVE-2006-3524 FULLDISC FULLDISC BID SECUNIA
Sport-slo -- Advanced Guestbook	Multiple cross-site scripting (XSS) vulnerabilities in guestbook.php in Sport-slo Advanced Guestbook 1.0 allow remote attackers to inject arbitrary web script or HTML via (1) name and (2) form parameters.	unknown 2006-07-11	4.7	CVE-2006-3526 BUGTRAQ FRSIRT SECUNIA

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
	** DISPUTED ** EMC VMware Player allows user-complicit attackers to cause a denial of service (unrecoverable application failure) via a long value of the ide1:0.fileName parameter in the .vmx file of a virtual machine. NOTE: third parties have disputed this issue, saying that write access to the .vmx file enables other ways of stopping the virtual machine, so no privilege boundaries are crossed.	unknown 2006-07-12	1.6	CVE-2006-3547 BUGTRAQ BUGTRAQ BUGTRAQ
Adobe -- Acrobat	Buffer overflow in Adobe Acrobat 6.0 to 6.0.4 allows remote attackers to execute arbitrary code via unknown vectors in a document that triggers the overflow when it is distilled to PDF.	unknown 2006-07-13	3.7	CVE-2006-3453 OTHER-REF FRSIRT SECTRACK SECUNIA XF
ATutor -- ATutor	Multiple cross-site scripting (XSS) vulnerabilities in ATutor before 1.5.3 allow remote attackers to inject arbitrary web script or HTML via the (1) show_courses or (2) current_cat parameters to (a) admin/create_course.php, show_courses parameter to (b) users/create_course.php, (3) p parameter to (c) documentation/admin/, (4) forgot parameter to (d) password_reminder.php, (5) cat parameter to (e) users/browse.php, or the (6) submit parameter to admin/fix_content.php.	unknown 2006-07-10	2.3	CVE-2006-3484 OTHER-REF BID FRSIRT SECUNIA
BT -- Voyager 2091 Wireless ADSL Router	BT Voyager 2091 Wireless firmware 2.21.05.08m_A2pB018c1.d16d and earlier, and 3.01m and earlier, allow remote attackers to bypass the authentication process and gain sensitive information, such as configuration information via (1) /btvoyager_getconfig.sh, PPP crendentials via (2) btvoyager_getpppcreds.sh, and decode configuration credentials via (3) btvoyager_decoder.c. NOTE: other refined sources have reported that "psiBackupInfo" and "connect.html" files are involved, but these vectors are not evident from the original disclosure.	unknown 2006-07-12	2.3	CVE-2006-3561 OTHER-REF FRSIRT SECUNIA
Clearswift -- MIMEsweeper for Web	Cross-site scripting (XSS) vulnerability in Clearswift MIMEsweeper for Web before 5.1.15 Hotfix allows remote attackers to inject arbitrary web script or HTML via the URL, which is reflected back in an error message when trying to access a blocked web site.	unknown 2006-07-11	2.3	CVE-2006-3522 FULLDISC FULLDISC FULLDISC OTHER-REF FRSIRT SECUNIA
Clearswift -- MIMEsweeper for Web	Clearswift MIMEsweeper for Web before 5.1.15 Hotfix allows remote attackers to cause a denial of service (crash) via an encrypted archived .RAR file, which triggers a scan error and causes the Web Policy Engine service to terminate.	unknown 2006-07-11	2.3	CVE-2006-3523 OTHER-REF FRSIRT SECUNIA
DKScript -- Dragon's Kingdom Script	Multiple cross-site scripting (XSS) vulnerabilities in DKScript.com Dragon's Kingdom Script 1.0 allow remote attackers to inject arbitrary web script or HTML via a javascript URI in the SRC attribute of an IMG element in the (1) Subject and (2) Message fields in a do=write (aka Send Mail Message) action in gamemail.php; the (3) Gender, (4) Country/Location, (5) MSN Messenger, (6) AOL Instant Messenger, (7) Yahoo Instant Messenger, and (8) ICQ fields in a do=onlinechar (aka Edit your Profile) action in index.php; a javascript URI in the SRC attribute of an IMG element in the (9) Title and	unknown 2006-07-12	2.3	CVE-2006-3539 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF

	(10) Message fields in a do=new (aka Create Thread) action in general.php; and a javascript URI in the SRC attribute of an IMG element in unspecified fields in (11) other Forum posts and (12) Forum replies.			OTHER-REF OTHER-REF FRSIRT SECUNIA
Drupal -- Drupal	Cross-site scripting (XSS) vulnerability in the webform module in Drupal 4.6 before July 8, 2006 and 4.7 before July 8, 2006 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2006-07-12	2.3	CVE-2006-3570 OTHER-REF FRSIRT SECUNIA
F-Secure -- Internet Security F-Secure -- Anti-Virus F-Secure -- Anti-Virus Client Security F-Secure -- Service Platform for Service Providers	F-Secure Anti-Virus 2003 through 2006 and other versions, Internet Security 2003 through 2006, and Service Platform for Service Providers 6.x and earlier allows remote attackers to bypass anti-virus scanning via a crafted filename.	unknown 2006-07-10	2.3	CVE-2006-3489 OTHER-REF FRSIRT SECTRACK SECTRACK
F-Secure -- Internet Security F-Secure -- Anti-Virus F-Secure -- Anti-Virus Client Security F-Secure -- Service Platform for Service Providers	F-Secure Anti-Virus 2003 through 2006 and other versions, Internet Security 2003 through 2006, and Service Platform for Service Providers 6.x and earlier does not scan files contained on removable media when "Scan network drives" is disabled, which allows remote attackers to bypass anti-virus controls.	unknown 2006-07-10	2.3	CVE-2006-3490 OTHER-REF FRSIRT SECTRACK SECTRACK OSVDB
F5 -- FirePass 4100	Multiple cross-site scripting (XSS) vulnerabilities in F5 Networks FirePass 4100 5.x allow remote attackers to inject arbitrary web script or HTML via unspecified "writable form fields and hidden fields," including "authentication frontends."	2006-06-08 2006-07-12	3.7	CVE-2006-3550 BUGTRAQ OTHER-REF BID FRSIRT SECTRACK
HiveMail -- HiveMail	Multiple cross-site scripting (XSS) vulnerabilities in HiveMail 1.3 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the email, (2) cond, or (3) name parameters to (a) addressbook.view.php, (4) the daysprune parameter to (b) index.php, (5) the data[to] parameter to (c) compose.email.php, and (6) the markas parameter to (d) read.markas.php.	unknown 2006-07-12	2.3	CVE-2006-3564 OTHER-REF SECUNIA
HiveMail -- HiveMail	search.results.php in HiveMail 3.1 and earlier allows remote attackers to obtain the installation path via certain manipulations related to the (1) searchdate and (2) folderids parameters.	unknown 2006-07-12	2.3	CVE-2006-3566 BLOGSPOT
Horde -- Horde	Multiple cross-site scripting (XSS) vulnerabilities in Horde Application Framework 3.0.0 through 3.0.10 and 3.1.0 through 3.1.1 allow remote attackers to inject arbitrary web script or HTML via a (1) javascript URI or an external (2) http, (3) https, or (4) ftp URI in the url parameter in services/go.php (aka the dereferrer), (5) a javascript URI in the module parameter in services/help (aka the help viewer), and (6) the name parameter in services/problem.php (aka the problem reporting screen).	2006-06-06 2006-07-12	2.3	CVE-2006-3548 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECTRACK
Horde -- Horde Application Framework	services/go.php in Horde Application Framework 3.0.0 through 3.0.10 and 3.1.0 through 3.1.1 does not properly restrict its image proxy capability, which allows remote attackers to perform "Web tunneling" attacks and use the server as a proxy via (1) http, (2) https, and (3) ftp URL in the url parameter, which is requested from the server.	unknown 2006-07-12	2.3	CVE-2006-3549 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECTRACK
ImgSvr -- ImgSvr	Patrice Freydiere ImgSvr (aka ADA Image Server) allows remote attackers to cause a denial of service (daemon crash) via a long HTTP POST request. NOTE: this might be the same issue as CVE-2004-2463.	unknown 2006-07-12	2.3	CVE-2006-3546 BUGTRAQ BID

Juniper -- JUNOS	Memory leak in Juniper JUNOS 6.4 through 8.0, built before May 10, 2006, allows remote attackers to cause a denial of service (kernel packet memory consumption and crash) via crafted IPv6 packets whose buffers are not released after they are processed.	unknown 2006-07-11	2.3	CVE-2006-3529 OTHER-REF CERT-VN
Juniper Networks -- DX	Cross-site scripting (XSS) vulnerability in the web administration interface logging feature in Juniper Networks (Redline) DX 5.1.x, and possibly earlier versions, allows remote attackers to inject arbitrary web script or HTML via the username login field.	unknown 2006-07-12	2.3	CVE-2006-3567 BUGTRAQ BID FRSIRT SECTRACK SECUNIA XF
Linux -- Linux kernel	The ftdi_sio driver (usb/serial/ftdi_sio.c) in Linux kernel 2.6.x up to 2.6.17, and possibly later versions, allows local users to cause a denial of service (memory consumption) by writing more data to the serial port than the driver can handle, which causes the data to be queued.	unknown 2006-07-10	2.3	CVE-2006-2936 OTHER-REF OTHER-REF
McAfee -- VirusScan	Unknown vulnerability in the Buffer Overflow Protection in McAfee VirusScan Enterprise 8.0.0 allows local users to cause a denial of service (unstable operation) via a long string in the (1) "Process name", (2) "Module name", or (3) "API name" fields.	unknown 2006-07-13	1.6	CVE-2006-3575 BUGTRAQ SECTRACK
MICO -- MICO	The CORBA::ORBInvokeRec::set_answer_invoke function in orb.cc in MICO (Mico Is CORBA) 2.3.12 and earlier allows remote attackers to cause a denial of service (application crash) via a message with an incorrect "object key", which triggers an assert error.	2006-06-27 2006-07-10	2.3	CVE-2006-3492 BUGTRAQ FRSIRT SECUNIA
Microsoft -- Office	Unspecified vulnerability in Microsoft Office 2003 SP1 and SP2, Office XP SP3, Office 2000 SP3, and other products, allows user-complicit attackers to execute arbitrary code via a crafted PNG image that triggers memory corruption when it is parsed.	unknown 2006-07-11	3.7	CVE-2006-0033 MS BID CERT-VN FRSIRT SECUNIA
Microsoft -- .NET Framework	Microsoft .NET framework 2.0 (ASP.NET) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 up to SP1 allows remote attackers to bypass access restrictions via unspecified "URL paths" that can access Application Folder objects "explicitly by name."	unknown 2006-07-11	2.3	CVE-2006-1300 MS BID FRSIRT SECTRACK SECUNIA XF
Microsoft -- Server Service	The Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to obtain sensitive information via crafted requests that leak information in SMB buffers, which are not properly initialized, aka "SMB Information Disclosure Vulnerability."	unknown 2006-07-11	2.3	CVE-2006-1315 MS BID XF
Microsoft -- Internet Explorer	Microsoft Internet Explorer 6 on Windows XP allows remote attackers to cause a denial of service (crash) via a table with a frameset as a child, which triggers a null dereference, as demonstrated using the appendChild method.	unknown 2006-07-10	2.3	CVE-2006-3471 OTHER-REF BID FRSIRT OSVDB
Microsoft -- Internet Explorer	Microsoft Internet Explorer 6.0 and 6.0 SP1 allows remote attackers to cause a denial of service via an HTML page with an A tag containing a long title attribute. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-07-10	2.3	CVE-2006-3472 BID
Microsoft -- Internet Explorer	The Remote Data Service Object (RDS.DataControl) in Microsoft Internet Explorer 6 on Windows 2000 allows remote attackers to cause a denial of service (crash) via a series of operations that result in an invalid length calculation when using SysAllocStringLen, then triggers a buffer over-read.	unknown 2006-07-11	1.9	CVE-2006-3510 OTHER-REF BID FRSIRT OSVDB XF
Microsoft -- Internet Explorer	Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) by setting the fonts property of the HtmlDlgSafeHelper object, which triggers a null dereference.	unknown 2006-07-11	2.3	CVE-2006-3511 OTHER-REF BID
Microsoft -- Internet Explorer	Internet Explorer 6 on Windows XP allows remote attackers to cause a denial of service (crash) by setting the Enabled property of a DXTFilter ActiveX object to true, which triggers a null dereference.	unknown 2006-07-11	2.3	CVE-2006-3512 BID FRSIRT XF

Microsoft -- Internet Explorer	danim.dll in Microsoft Internet Explorer 6 allows remote attackers to cause a denial of service (application crash) by accessing the Data property of a DirectAnimation DAUserData object before it being initialized, which triggers a NULL pointer dereference.	unknown 2006-07-11	2.3	CVE-2006-3513 OTHER-REF BID FRSIRT
Microsoft -- Internet Explorer	** DISPUTED ** Microsoft Internet Explorer 7.0 Beta allows remote attackers to cause a denial of service (application crash) via a web page with multiple empty APPLET start tags. NOTE: a third party has disputed this issue, stating that the crash does not occur with Microsoft Internet Explorer 7.0 Beta3.	unknown 2006-07-12	2.3	CVE-2006-3545 BUGTRAQ BUGTRAQ
MT Orumcek -- Toplist	MT Orumcek Toplist 2.2 stores DB/orumcektoplist.mdb under the web root with insufficient access control, which allows remote attackers to obtain sensitive information via a direct request.	unknown 2006-07-12	2.3	CVE-2006-3557 BUGTRAQ
MySQL -- MySQL	Off-by-one buffer overflow in the Instance_options::complete_initialization function in instance_options.cc in the Instance Manager in MySQL before 5.0.23 and 5.1 before 5.1.12 might allow local users to cause a denial of service (application crash) via unspecified vectors, which triggers the overflow when the convert_dirname function is called.	unknown 2006-07-10	1.6	CVE-2006-3486 OTHER-REF OTHER-REF OTHER-REF FRSIRT
NCP Network Communications -- Secure Client	NCP Secure Enterprise Client (aka VPN/PKI client) 8.30 Build 59, and possibly earlier versions, when the Link Firewall and Personal Firewall are both configured to block all inbound and outbound network traffic, allows context-dependent attackers to send inbound UDP traffic with source port 67 and destination port 68, and outbound UDP traffic with source port 68 and destination port 67.	2006-05-12 2006-07-12	1.3	CVE-2006-3551 FULLDISC XF
Nuked-Klan -- Nuked-Klan	Cross-site request forgery (CSRF) vulnerability in the del_block function in modules/Admin/block.php in Nuked-Klan 1.7.5 and earlier and 1.7 SP4.2 allows remote attackers to delete arbitrary "blocks" via a link with a modified bid parameter in a del_block op on the block page in index.php.	unknown 2006-07-10	2.3	CVE-2006-3479 BUGTRAQ FRSIRT SECUNIA XF
Nullsoft -- SHOUTcast Server	Directory traversal vulnerability in Nullsoft SHOUTcast DSP before 1.9.6 filters directory traversal sequences before decoding, which allows remote attackers to read arbitrary files via encoded dot dot (%2E%2E) sequences in an HTTP GET request for a file path containing "/content".	2006-06-13 2006-07-12	3.3	CVE-2006-3534 GENTOO OTHER-REF SHOUTCAST GENTOO SECUNIA
NullSoft -- Shoutcast DSP	Directory traversal vulnerability in Nullsoft SHOUTcast DSP before 1.9.7 allows remote attackers to read arbitrary files via unspecifed vectors, which are a "slight variation" of CVE-2006-????.	unknown 2006-07-12	2.3	CVE-2006-3535 OTHER-REF OTHER-REF OTHER-REF GENTOO SECUNIA
Papoo -- Papoo	Multiple cross-site scripting (XSS) vulnerabilities in interna/hilfe.php in Papoo 3 RC3 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) titel or (2) parameters.	unknown 2006-07-12	2.3	CVE-2006-3571 BUGTRAQ OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
PHP-Blogger -- PHP-Blogger	Multiple cross-site scripting (XSS) vulnerabilities in admin/actions.php in PHP-Blogger 2.2.5, and possibly earlier versions, allow remote attackers to execute arbitrary web script or HTML via the (1) name, (2) title, (3) news, (4) description, and (5) sitename parameters.	2006-06-14 2006-07-11	2.3	CVE-2006-3514 BUGTRAQ FRSIRT
PHPMailList -- PHPMailList	PHPMailList 1.8.0 stores sensitive information under the web document root iwth insufficient access control, which allows remote attackers to obtain email addresses of subscribers, configuration information, and the admin username and password via direct requests to (1) list.dat or (2) ml_config.dat.	unknown 2006-07-10	2.3	CVE-2006-3483 OTHER-REF SECTRACK
PhpWebGallery -- PhpWebGallery	Cross-site scripting (XSS) vulnerability in comments.php in PhpWebGallery 1.5.2 and earlier, and possibly 1.6.0, allows remote attackers to inject arbitrary web script or HTML via the keyword parameter.	unknown 2006-07-10	2.3	CVE-2006-3476 BUGTRAQ BID FRSIRT SECUNIA
Qbik -- WinGate	Directory traversal vulnerability in the IMAP server in WinGate 6.1.2.1094 and 6.1.3.1096, and possibly other versions before 6.1.4 Build 1099, allows remote authenticated users to read email of other users, or perform unauthorized operations on	2006-06-16 2006-07-10	2.8	CVE-2006-2917 OTHER-REF SECUNIA

	directories, via the (1) CREATE, (2) SELECT, (3) DELETE, (4) RENAME, (5) COPY, (6) APPEND, and (7) LIST commands.			OTHER-REF BID FRSIRT
Samba -- Samba	The smdb daemon (smbd/service.c) in Samba 3.0.1 through 3.0.22 allows remote attackers to cause a denial of service (memory consumption) via a large number of share connection requests.	unknown 2006-07-12	2.3	CVE-2006-3403 OTHER-REF MANDRIVA BID FRSIRT SECUNIA SECUNIA
Stalker -- Communigate	Unspecified vulnerability in the POP service in Stalker CommuniGate Pro 5.1c1 and earlier allows remote attackers to cause a denial of service (server crash) via unspecified vectors involving opening an empty inbox.	unknown 2006-07-10	2.3	CVE-2006-3477 OTHER-REF BID FRSIRT SECUNIA XF
VirtuaStore -- VirtuaStore	VirtuaStore 2.0 stores sensitive files under the web root with insufficient access control, which allows remote attackers to obtain local database information by directly accessing database/virtuastore.mdb.	unknown 2006-07-10	2.3	CVE-2006-3487 SECTRACK
VirtuaStore -- VirtuaStore	Absolute path traversal vulnerability in administrador.asp in VirtuaStore 2.0 allows remote attackers to possibly read arbitrary directories or files via an absolute path with Windows drive letter in the Pasta parameter when link=util, acao=ftp, and acaba=sim.	unknown 2006-07-10	2.3	CVE-2006-3488 SECTRACK
Winged Gallery -- Winged Gallery	Cross-site scripting (XSS) vulnerability in gallery/thumb.php in Winged Gallery 1.0 allows remote attackers to inject arbitrary web script or HTML via the image parameter.	unknown 2006-07-12	2.3	CVE-2006-3563 BUGTRAQ BID XF
Zone Labs -- ZoneAlarm Internet Security Suite	Check Point Zone Labs ZoneAlarm Internet Security Suite 6.5.722.000, 6.1.737.000, and possibly other versions do not properly validate RegSaveKey, RegRestoreKey, and RegDeleteKey function calls, which allows local users to cause a denial of service (system crash) via a certain combination of these function calls with an HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VETFDDNT\Enum argument.	unknown 2006-07-12	1.6	CVE-2006-3540 BUGTRAQ OTHER-REF BID
Zope -- Zope	Unspecified vulnerability in Zope 2.7.0 to 2.7.8, 2.8.0 to 2.8.7, and 2.9.0 to 2.9.3 (Zope2) allows local users to obtain sensitive information via unknown attack vectors related to the docutils module and "restructured text".	unknown 2006-07-07	1.6	CVE-2006-3458 OTHER-REF SECUNIA

Back to top

Last updated July 17, 2006