




[Advanced Options...](#)

National Cyber Alert System

Cyber Security Bulletin SB06-296

[Archive](#)

Vulnerability Summary for the Week of October 16, 2006

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
				CVE-2006-

AFGB -- AFGB Guestbook	Multiple PHP remote file inclusion vulnerabilities in AFGB GUESTBOOK 2.2 allow remote attackers to execute arbitrary PHP code via a URL in the Htmls parameter in (1) add.php, (2) admin.php, (3) look.php, or (4) re.php.	unknown 2006-10-17	7.0	5307 Milw0rm BID SECUNIA XF
Alex -- DownloadEngine	PHP remote file inclusion vulnerability in admin/includes/spaw/spaw_control.class.php in Download-Engine 1.4.2 allows remote attackers to execute arbitrary PHP code via a URL in the spaw_root parameter.	unknown 2006-10-16	7.0	CVE-2006- 5291 BUGTRAQ Milw0rm BID FRSIRT SECUNIA XF
Apple -- Xcode Tools Openbase International Ltd -- OpenBase	Untrusted search path vulnerability in OpenBase SQL 10.0 and earlier, as used in Apple Xcode 2.2 2.2 and earlier and possibly other products, allows local users to execute arbitrary code via a modified PATH that references a malicious gzip program, which is executed by gnutar with certain TAR_OPTIONS environment variable settings, when gnutar is invoked by OpenBase.	unknown 2006-10-17	7.0	CVE-2006- 5327 OTHER- REF OTHER- REF BID SECUNIA FRSIRT FRSIRT SECUNIA
Apple -- Xcode Tools Openbase International Ltd -- OpenBase	OpenBase SQL 10.0 and earlier, as used in Apple Xcode 2.2 2.2 and earlier and possibly other products, allows local users to create arbitrary files via a symlink attack on the simulation.sql file.	unknown 2006-10-17	7.0	CVE-2006- 5328 OTHER- REF OTHER- REF BID SECUNIA
				CVE-2006-

AROUNDMe -- AROUNDMe	PHP remote file inclusion vulnerability in template/barnraiser_01/p_new_password.tpl.php in AROUNDMe 0.5.2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the templatePath parameter.	unknown 2006-10-18	7.0	5401 OTHER- REF BID XF
Barry Nauta -- BRIM	Multiple PHP remote file inclusion vulnerabilities in Barry Nauta BRIM 1.2.1 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the renderer parameter in template.tpl.php in (1) templates/barrel/, (2) templates/sidebar/, (3) templates/text-only, (4) templates/slashdot/, (5) templates/penguin/, (6) templates/pda/, (7) templates/oerdec/, (8) templates/nifty/, (9) templates/mylook, and (10) templates/barry/.	unknown 2006-10-20	7.0	CVE-2006- 5429 OTHER- REF BID FRSIRT SECUNIA XF
Buzlas -- Buzlas	PHP remote file inclusion vulnerability in includes/archive/archive_topic.php in Buzlas 2006-1 Full allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	unknown 2006-10-17	7.0	CVE-2006- 5311 BUGTRAQ BID
CDS Software Consortium -- CDS Agenda	PHP remote file inclusion vulnerability in modification/SendAlertEmail.php in CDS Software Consortium CDS Agenda 4.2.9 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the AGE parameter.	unknown 2006-10-18	7.0	CVE-2006- 5384 OTHER- REF BID FRSIRT SECUNIA XF
Cerberus -- Helpdesk	rpc.php in Cerberus Helpdesk 3.2.1 does not verify a client's privileges for a display_get_requesters operation, which allows remote attackers to bypass the GUI login and obtain sensitive information (ticket data) via a direct request.	unknown 2006-10-20	7.0	CVE-2006- 5428 OTHER- REF BID FRSIRT SECUNIA

Clam Anti-Virus -- ClamAV	Integer overflow in ClamAV 0.88.1 and 0.88.4, and other versions before 0.88.5, allows remote attackers to cause a denial of service (scanning service crash) and execute arbitrary code via a crafted Portable Executable (PE) file that leads to a heap-based buffer overflow when less memory is allocated than expected.	2006-08-16 2006-10-16	7.0	CVE-2006-4182 IDEFENSE BID FRSIRT SECUNIA
Contenido -- Contendio	** DISPUTED ** Remote file inclusion vulnerability in Contenido CMS allows remote attackers to execute arbitrary PHP code via a URL in the contenido_path parameter to (1) cms/dbfs.php or (2) cms/front_content.php. NOTE: CVE disputes this issue for version 4.6.15, because \$contenido_path is set to a static value.	unknown 2006-10-18	7.0	CVE-2006-5380 BUGTRAQ MLIST XF
Def-Blog -- Def-Blog	SQL injection vulnerability in comadd.php in Def-Blog 1.0.1 and earlier allows remote attackers to execute arbitrary SQL commands via the article parameter.	unknown 2006-10-18	7.0	CVE-2006-5383 OTHER-REF BID FRSIRT SECUNIA XF
Dimitri Seitz -- Security Suite IP Logger	Multiple PHP remote file inclusion vulnerabilities in Dimitri Seitz Security Suite IP Logger in dwingmods for phpBB allow remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter in (1) mkb.php, (2) iplogger.php, (3) admin_board2.php, or (4) admin_logger.php in includes/, different vectors than CVE-2006-5224.	unknown 2006-10-17	7.0	CVE-2006-5325 BUGTRAQ
Exhibit Engine -- Exhibit Engine	PHP remote file inclusion vulnerability in photo_comment.php in Exhibit Engine 1.5 RC 4 and earlier allows remote attackers to execute arbitrary	unknown 2006-10-16	7.0	CVE-2006-5292 OTHER-REF

	PHP code via a URL in the toroot parameter.			BID XF
Highwall -- Highwall Endpoint Highwall -- Highwall Enterprise	Multiple SQL injection vulnerabilities in the wireless IDS management interface for Highwall Enterprise and Highwall Endpoint 4.0.2.11045 allow remote attackers to execute arbitrary SQL commands via unspecified vectors.	unknown 2006-10-20	7.0	CVE-2006-5409 BUGTRAQ BID
IBM -- Websphere Application Server	The Web Services Notification (WSN) security component of IBM WebSphere Application Server before 6.1.0.2 allows attackers to obtain unspecified access without supplying a username and password, aka PK28374.	unknown 2006-10-17	7.0	CVE-2006-5324 OTHER-REF OTHER-REF AIXAPAR FRSIRT SECUNIA
IncCMS Technology -- IncCMS Core	PHP remote file inclusion vulnerability in inc/settings.php in IncCMS Core 1.0.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the inc_dir parameter.	unknown 2006-10-17	7.0	CVE-2006-5304 OTHER-REF OTHER-REF BID SECUNIA
jhjgubbels -- eboli	PHP remote file inclusion vulnerability in index.php in eboli allows remote attackers to execute arbitrary PHP code via a URL in the contentSpecial parameter.	unknown 2006-10-17	7.0	CVE-2006-5317 BUGTRAQ ACID-ROOT Milw0rm BID
				CVE-2006-

Justin White -- FreeWPS	Unrestricted file upload vulnerability in upload.php for Free Web Publishing System (FreeWPS), possibly 2.11 and earlier, allows remote attackers to upload and execute arbitrary PHP programs.	unknown 2006-10-20	7.0	5411 BUGTRAQ BID SECUNIA XF
KDE -- kdelibs	Integer overflow in Qt, as used in the KDE khtml library, kdelibs 3.1.3, and possibly other packages, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted pixmap image.	unknown 2006-10-18	8.0	CVE-2006-4811 REDHAT OTHER- REF
LoCal Calendar System -- LoCal Calendar System	PHP remote file inclusion vulnerability in lib/lcUser.php in LoCal Calendar System 1.1 remote attackers to execute arbitrary PHP code via a URL in the LIBDIR parameter.	unknown 2006-10-20	7.0	CVE-2006-5426 OTHER- REF BID FRSIRT SECUNIA
Lodel -- Lodel CMS	PHP remote file inclusion vulnerability in calcul-page.php in Lodel (patchlodel) 0.7.3 allows remote attackers to execute arbitrary PHP code via a URL in the home parameter.	unknown 2006-10-20	7.0	CVE-2006-5422 BUGTRAQ BID FRSIRT SECUNIA XF
Lou Portail -- Lou Portail	PHP remote file inclusion vulnerability in admin/admin_module.php in Lou Portail 1.4.1, and possibly earlier, allows remote attackers to execute arbitrary PHP code via a URL in the g_admin_rep parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-10-20	7.0	CVE-2006-5423 BID FRSIRT SECUNIA
	Buffer overflow in Microsoft Class Package Export Tool			

Microsoft -- Class Package Export Tool	(aka clspack.exe) allows context-dependent attackers to execute arbitrary code via a long string. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-10-18	7.0	CVE-2006-5395 BID
Minichat -- Minichat	PHP remote file inclusion vulnerability in ftag.php in Minichat 6.0 allows remote attackers to execute arbitrary PHP code via a URL in the mostrar parameter.	unknown 2006-10-13	7.0	CVE-2006-5283 Milw0rm FRSIRT SECUNIA XF
navyism -- n@board	PHP remote file inclusion vulnerability in nboard_pnr.php in n@board 3.1.9e and earlier allows remote attackers to execute arbitrary PHP code via a URL in the skin parameter.	unknown 2006-10-13	7.0	CVE-2006-5281 Milw0rm FRSIRT SECUNIA XF
Nayco -- JASmine	PHP remote file inclusion vulnerability in index.php in Nayco JASmine (aka Jasmine-Web) allows remote attackers to execute arbitrary PHP code via an FTP URL in the section parameter.	unknown 2006-10-17	7.0	CVE-2006-5318 BUGTRAQ OTHER-REF OTHER-REF BID SECUNIA XF FRSIRT
News Defilante Horizontale -- News Defilante Horizontale	PHP remote file inclusion vulnerability in includes/functions_newshr.php in the News Defilante Horizontale 4.1.1 and earlier module for phpBB allows remote attackers to execute arbitrary PHP code via a	unknown 2006-10-20	7.0	CVE-2006-5415 BUGTRAQ OTHER-REF BID

	URL in the phpbb_root_path parameter.			FRSIRT SECUNIA XF
NuralStorm -- NuralStorm Webmail	PHP remote file inclusion vulnerability in process.php in NuralStorm Webmail 0.98b and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the DEFAULT_SKIN parameter.	unknown 2006-10-18	7.0	CVE-2006-5386 OTHER- REF FRSIRT SECUNIA XF
Nvidia -- Binary Graphics Driver	The accelerated rendering functionality of NVIDIA Binary Graphics Driver (binary blob driver) For Linux v8774 and v8762, and probably on other operating systems, allows local and remote attackers to execute arbitrary code via a large width value in a font glyph, which can be used to overwrite arbitrary memory locations.	unknown 2006-10-18	7.0	CVE-2006-5379 BUGTRAQ OTHER- REF OTHER- REF CERT-VN FRSIRT SECTRACK SECUNIA
Open Conference Systems -- Open Conference Systems	Multiple PHP remote file inclusion vulnerabilities in Open Conference Systems (OCS) before 1.1.6 allow remote attackers to execute arbitrary PHP code via a URL in the fullpath parameter in (1) include/theme.inc.php or (2) include/footer.inc.php.	unknown 2006-10-17	7.0	CVE-2006-5308 OTHER- REF OTHER- REF OTHER- REF OTHER- REF OTHER- REF

				SECUNIA XF BID FRSIRT SECTRACK
OpenDoc -- FullCore	Multiple PHP remote file inclusion vulnerabilities in OpenDock FullCore 4.4 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the doc_directory parameter in (1) sw/index_sw.php; (2) cart.php, (3) lib_cart.php, (4) lib_read_cart.php, (5) lib_sys_cart.php, and (6) txt_info_cart.php in sw/lib_cart/; (7) comment.php, (8) find_comment.php, and (9) lib_comment.php in sw/lib_comment/; (10) sw/lib_find/find.php; and other unspecified PHP scripts.	unknown 2006-10-18	7.0	CVE-2006-5392 OTHER-REF BID FRSIRT XF
Oracle -- Oracle HTTP Server	Unspecified vulnerability in Oracle HTTP Server 9.2.0.7 and Oracle Collaboration Suite 9.0.4.2 has unknown impact and remote attack vectors related to HTTPS and SSL, aka Vuln# OHS04.	unknown 2006-10-17	7.0	CVE-2006-5347 ORACLE BID FRSIRT
Oracle -- Oracle E-Business Suite and Applications Oracle -- Oracle Collaboration Suite Oracle -- Oracle HTTP Server	Unspecified vulnerability in Oracle HTTP Server 9.2.0.7, Oracle Collaboration Suite 9.0.4.2, and Oracle E-Business Suite and Applications 11.5.10CU2 has unknown impact and remote attack vectors related to HTTPS and SSL, aka Vuln# OHS05.	unknown 2006-10-17	7.0	CVE-2006-5348 ORACLE BID FRSIRT
Oracle -- Oracle HTTP Server	Unspecified vulnerability in Oracle HTTP Server 9.2.0.7, when running on HP Tru64 UNIX, has unknown impact and remote attack vectors related to HTTPS and SSL, aka Vuln# OHS07.	unknown 2006-10-17	7.0	CVE-2006-5349 OTHER-REF BID FRSIRT

Oracle -- Application Express	Multiple unspecified vulnerabilities in Oracle Application Express (formerly Oracle HTML DB) 1.5 up to 2.0 have unknown impact and remote attack vectors, aka Vuln# (1) APEX01, (2) APEX02, (3) APEX03, (4) APEX05, (5) APEX06, (6) APEX07, (7) APEX08, (8) APEX09, (9) APEX10, (10) APEX11, (11) APEX12, (12) APEX13, (13) APEX14, (14) APEX15, (15) APEX16, (16) APEX17, (17) APEX18, (18) APEX19, (19) APEX22, (20) APEX23, (21) APEX24, (22) APEX25, (23) APEX26, (24) APEX27, (25) APEX28, (26) APEX29, (27) APEX30, (28) APEX31, (29) APEX32, (30) APEX33, (31) APEX34, and (32) APEX35.	unknown 2006-10-17	7.0	CVE-2006-5351 OTHER-REF BID FRSIRT
Oracle -- Application Express	Multiple unspecified vulnerabilities in Oracle Application Express 1.5 up to 1.6.1 have unknown impact and remote attack vectors, aka Vuln# (1) APEX04, (2) APEX20, and (3) APEX21.	unknown 2006-10-17	7.0	CVE-2006-5352 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g Oracle -- Oracle Collaboration Suite	Unspecified vulnerability in Oracle HTTP Server component in Oracle Application Server 9.0.4.3, 10.1.2.0.2, 10.1.2.1.0, and 10.1.3.0.0, and Oracle Collaboration Suite 9.0.4.2 and 10.1.2, has unknown impact and remote attack vectors related to the Mod_rewrite Module, aka Vuln# OHS01.	unknown 2006-10-17	7.0	CVE-2006-5353 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g Oracle -- Oracle Collaboration Suite Oracle -- Oracle HTTP Server Oracle -- E-Business Suite	Unspecified vulnerability in Oracle HTTP Server 9.2.0.7 and 10.1.0.5, Application Server 9.0.4.3, 10.1.2.0.2, 10.1.2.1.0, and 10.1.3.0, Oracle Collaboration Suite 9.0.4.2 and 10.1.2, and Oracle E-Business Suite and Applications 11.5.10CU2 has unknown impact and remote attack vectors, aka Vuln# OHS06.	unknown 2006-10-17	7.0	CVE-2006-5354 OTHER-REF BID FRSIRT

Oracle -- Application Server 10g Oracle -- Oracle Collaboration Suite Oracle -- E-Business Suite	Unspecified vulnerability in Oracle Single Sign-On component in Oracle Application Server 9.0.4.3, 10.1.2.0.2, and 10.1.2.1.0, Collaboration Suite 9.0.4.2 and 10.1.2, and Oracle E-Business Suite and Applications 11.5.10CU2 has unknown impact and remote attack vectors, aka Vuln# SSO01.	unknown 2006-10-17	7.0	CVE-2006-5355 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g Oracle -- Oracle Collaboration Suite	Unspecified vulnerability in Oracle Containers for J2EE component in Oracle Application Server 9.0.4.3, 10.1.2.0.2, and 10.1.2.1.0, and Collaboration Suite 9.0.4.2 and 10.1.2, has unknown impact and remote attack vectors, aka Vuln# OC4J02.	unknown 2006-10-17	7.0	CVE-2006-5356 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g	Unspecified vulnerability in Oracle HTTP Server component in Oracle Application Server 10.1.2.0.1, 10.1.2.0.2, and 10.1.2.1.0 has unknown impact and remote attack vectors related to the PHP Module, aka Vuln# OHS03.	unknown 2006-10-17	7.0	CVE-2006-5357 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g	Unspecified vulnerability in Oracle Forms component in Oracle Application Server 9.0.4.3 and 10.1.2.0.2 has unknown impact and remote attack vectors, aka Vuln# FORM01.	unknown 2006-10-17	7.0	CVE-2006-5358 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g Oracle -- E-Business Suite	Multiple unspecified vulnerabilities in Oracle Reports Developer component in Oracle Application Server 9.0.4.3 and 10.1.2.0.2, and Oracle E-Business Suite and Applications 11.5.10CU2, have unknown impact and remote attack vectors, aka Vuln# (1) REP01 and (2) REP02.	unknown 2006-10-17	7.0	CVE-2006-5359 OTHER-REF BID FRSIRT
	Unspecified vulnerability in Oracle Forms component			CVE-2006-5360

Oracle -- Application Server 10g	in Oracle Application Server 9.0.4.2 has unknown impact and remote attack vectors, aka Vuln# FORM03.	unknown 2006-10-17	7.0	OTHER-REF BID FRSIRT
Oracle -- Application Server 10g Oracle -- Oracle Collaboration Suite	Unspecified vulnerability in Oracle Containers for J2EE in Oracle Application Server 9.0.4.3, 10.1.2.0.0, and 10.1.2.0.1, and Oracle Collaboration Suite 9.0.4.2 and 10.1.2, has unknown impact and remote attack vectors, aka Vuln# OC4J03.	unknown 2006-10-17	7.0	CVE-2006-5361 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g	Unspecified vulnerability in Oracle Containers for J2EE component in Oracle Application Server 10.1.3.0.0 has unknown impact and remote attack vectors, aka Vuln# OC4J04.	unknown 2006-10-17	7.0	CVE-2006-5362 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g Oracle -- Oracle Collaboration Suite	Unspecified vulnerability in Oracle Single Sign-On component in Oracle Application Server 10.1.2.0.1 and Oracle Collaboration Suite 10.1.2 has unknown impact and remote attack vectors, aka Vuln# SSO02.	unknown 2006-10-17	7.0	CVE-2006-5363 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g Oracle -- Oracle Collaboration Suite	Unspecified vulnerability in Oracle Containers for J2EE component in Oracle Application Server 9.0.4.1 and 10.1.2.0.2, and Oracle Collaboration Suite 10.1.2, has unknown impact and remote authenticated attack vectors, aka Vuln# OC4J05.	unknown 2006-10-17	7.0	CVE-2006-5364 OTHER-REF BID FRSIRT
Oracle -- Application Server 10g Oracle -- E-Business	Unspecified vulnerability in Oracle Forms in Oracle Application Server 9.0.4.3 and 10.1.2.0.2, and E-Business Suite and Applications 11.5.10CU2, has unknown impact and remote attack vectors, aka Vuln#	unknown 2006-10-17	7.0	CVE-2006-5365 OTHER-REF

Suite	FORM02.			BID FRSIRT
Oracle -- Application Server 10g	Multiple unspecified vulnerabilities in Oracle Collaboration Suite 9.0.4.2 have unknown impact and remote attack vectors related to (1) Oracle Containers for J2EE, aka Vuln# OC4J01, and (2) Oracle Process Mgmt & Notification, aka OPMN01.	unknown 2006-10-17	7.0	CVE-2006-5366 OTHER-REF BID FRSIRT
Oracle -- E-Business Suite	Unspecified vulnerability in Oracle Exchange component in Oracle E-Business Suite 6.2.4 has unknown impact and remote attack vectors, aka Vuln# APPS01.	unknown 2006-10-17	7.0	CVE-2006-5368 OTHER-REF BID FRSIRT
Oracle -- E-Business Suite	Unspecified vulnerability in Oracle Application Object Library in Oracle E-Business Suite 11.5.10CU2 has unknown impact and remote authenticated attack vectors, aka Vuln# APPS02.	unknown 2006-10-17	7.0	CVE-2006-5369 OTHER-REF BID FRSIRT
Oracle -- E-Business Suite	Multiple unspecified vulnerabilities in Oracle E-Business Suite 11.5.10CU2 have unknown impact and remote authenticated attack vectors, aka Vuln# (1) APPS06 for Oracle CRM Gateway for Mobile Devices and (2) APPS08 for Oracle iStore.	unknown 2006-10-17	7.0	CVE-2006-5370 OTHER-REF BID FRSIRT
Oracle -- Pharmaceutical Applications	Unspecified vulnerability in Oracle Pharmaceutical Applications 4.5.1 has unknown impact and remote authenticated attack vectors, aka Vuln# PHAR01.	unknown 2006-10-17	7.0	CVE-2006-5374 OTHER-REF BID FRSIRT

Oracle -- Oracle PeopleSoft Enterprise	Multiple unspecified vulnerabilities in PeopleTools component in Oracle PeopleSoft Enterprise 8.46 GA, 8.47 GA, 8.48 GA, 8.46.15, 8.47.09, and 8.48.03 have unknown impact and remote attack vectors, aka Vuln# (1) PSE01, (2) PSE02, and (3) PSE03.	unknown 2006-10-17	7.0	CVE-2006-5375 OTHER-REF BID FRSIRT
osTicket -- osTicket	PHP remote file inclusion vulnerability in open_form.php in osTicket allows remote attackers to execute arbitrary PHP code via a URL in the include_dir parameter.	unknown 2006-10-18	7.0	CVE-2006-5407 BUGTRAQ XF
phpBB -- Journals System module	Multiple PHP remote file inclusion vulnerabilities in the Journals System module 1.0.2 (RC2) and earlier for phpBB allow remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter in (1) includes/journals_delete.php, (2) includes/journals_post.php, or (3) includes/journals_edit.php.	unknown 2006-10-17	7.0	CVE-2006-5306 BUGTRAQ Milw0rm BID FRSIRT SECTRACK SECUNIA XF
phpBB -- Prillian French	PHP remote file inclusion vulnerability in language/lang_french/lang_prillian_faq.php in the Prillian French 0.8.0 and earlier module for phpBB allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	unknown 2006-10-17	7.0	CVE-2006-5309 BUGTRAQ Milw0rm BID FRSIRT SECUNIA XF
phpBB -- Ajax Shoutbox	PHP remote file inclusion vulnerability in shoutbox.php in the Ajax Shoutbox 0.0.5 and earlier module for phpBB allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	unknown 2006-10-17	7.0	CVE-2006-5312 Milw0rm XF

phpBB -- ACP User Registration Module	PHP remote file inclusion vulnerability in includes/functions_mod_user.php in the ACP User Registration (MMW) 1.00 module for phpBB allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	unknown 2006-10-18	7.0	CVE-2006-5390 Milw0rm OTHER-REF BID SECUNIA XF
phpBB -- SearchIndexer	PHP remote file inclusion vulnerability in archive/archive_topic.php in pbpb archive for search engines (SearchIndexer) (aka phpBBSEI) for phpBB allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	unknown 2006-10-20	7.0	CVE-2006-5418 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA XF
phpBB PlusXL -- PlusXL	PHP remote file inclusion vulnerability in mods/iai/includes/constants.php in the PlusXL 20_272 and earlier phpBB module allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	unknown 2006-10-18	7.0	CVE-2006-5387 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA XF
phpBB Prillian -- French Language Pack	PHP remote file inclusion vulnerability in language/lang/lang_contact_faq.php in the Prillian French 0.8.0 and earlier module for phpBB allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-10-17	7.0	CVE-2006-5326 FRSIRT SECUNIA

phpLibre -- TribunaLibre	PHP remote file inclusion vulnerability in ftag.php in TribunaLibre 3.12 Beta allows remote attackers to execute arbitrary PHP code via a URL in the mostrar parameter.	unknown 2006-10-17	7.0	CVE-2006-5314 BUGTRAQ ACID-ROOT Milw0rm XF
phpLibre -- RegistroTL	PHP remote file inclusion vulnerability in main.php in registroTL allows remote attackers to execute arbitrary PHP code via an ftp:// URL in the page parameter.	unknown 2006-10-17	7.0	CVE-2006-5315 BUGTRAQ ACID-ROOT Milw0rm BID XF
PHPmybibli -- PHPmybibli	Multiple PHP remote file inclusion vulnerabilities in PHPmybibli 2.1 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the (1) class_path, (2) javascript_path, and (3) include_path parameters in (a) cart.php; the (4) class_path parameter in (b) index.php; the (5) javascript_path parameter in (c) edit.php; the (6) include_path parameter in (d) circ.php; unspecified parameters in (e) select.php; and unspecified parameters in other files.	unknown 2006-10-18	7.0	CVE-2006-5402 BUGTRAQ OTHER-REF BID
phpMyConferences -- phpMyConferences	PHP remote file inclusion vulnerability in common/visiteurs/include/menus.inc.php in phpMyConferences (phpMyConference) 8.0.2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the lvc_include_dir parameter.	unknown 2006-10-17	7.0	CVE-2006-5310 BUGTRAQ Milw0rm XF FRSIRT SECUNIA
				CVE-2006-5293

PhpOutsourcing -- Noah's Classifieds	Cross-site scripting (XSS) vulnerability in index.php in PhpOutsourcing Noah's Classifieds 1.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the frommethod parameter.	unknown 2006-10-16	7.0	BUGTRAQ OTHER- REF BID XF
PHPOutsourcing -- Zorum	PHP remote file inclusion vulnerability in gorum/dbproperty.php in PHPOutsourcing Zorum 3.5 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the appDirName parameter.	unknown 2006-10-20	7.0	CVE-2006- 5431 BUGTRAQ BID XF
PHPRecipeBook -- PHPRecipeBook	PHP remote file inclusion vulnerability in classes/Import_MM.class.php in PHPRecipeBook 2.36, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the g_rb_basedir parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-10-18	7.0	CVE-2006- 5399 FRSIRT SECUNIA
Redaction System -- Redaction System	Multiple PHP remote file inclusion vulnerabilities in Redaction System 1.0000 allow remote attackers to execute arbitrary PHP code via a URL in the (1) lang_prefix parameter to (a) conn.php, (b) sesscheck.php, (c) wap/conn.php, or (d) wap/sesscheck.php, or the (2) lang parameter to (d) index.php.	unknown 2006-10-17	7.0	CVE-2006- 5302 OTHER- REF OTHER- REF OTHER- REF BID FRSIRT SECUNIA XF
SH-News -- SH-News	Multiple PHP remote file inclusion vulnerabilities in SH-News 3.1 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the scriptpath	unknown	7.0	CVE-2006- 5282 MilwOrm BID

	parameter to (1) report.php, (2) archive.php, (3) comments.php, (4) init.php, or (5) news.php.	2006-10-13		FRSIRT SECUNIA XF
Simplog -- Simplog	SQL injection vulnerability in comments.php in Simplog 0.9.3.1 allows remote attackers to execute arbitrary SQL commands via the cid parameter.	unknown 2006-10-18	7.0	CVE-2006-5398 OTHER- REF BID XF
SpamOborona -- SpamOborona	PHP remote file inclusion vulnerability in admin/admin_spam.php in the SpamOborona 1.0b and earlier phpBB module allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	unknown 2006-10-18	7.0	CVE-2006-5385 BUGTRAQ OTHER- REF BID FRSIRT SECUNIA XF
SuperMod -- SuperMod	Multiple PHP remote file inclusion vulnerabilities in SuperMod 3.0.0 for YABB (YaBBSM) allow remote attackers to execute arbitrary PHP code via a URL in the sourcedir parameter to (1) Offline.php, (2) Sources/Admin.php, (3) Sources/Offline.php, or (4) content/portalshow.php.	unknown 2006-10-20	7.0	CVE-2006-5413 OTHER- REF BID BID FRSIRT SECUNIA XF
tincan -- PHPList	Multiple SQL injection vulnerabilities in phplist before 2.10.3 allow remote attackers to execute arbitrary SQL commands via unspecified vectors.	unknown 2006-10-17	7.0	CVE-2006-5322 OTHER- REF OTHER- REF

University of Glasgow - - Specimen Image Database	PHP remote file inclusion vulnerability in client.php in University of Glasgow Specimen Image Database (SID), when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the dir parameter.	unknown 2006-10-20	7.0	CVE-2006-5419 OTHER-REF BID FRSIRT SECUNIA XF
webSPELL -- webSPELL	SQL injection vulnerability in index.php in WebSPELL 4.01.01 and earlier allows remote attackers to execute arbitrary SQL commands via the getsquad parameter, a different vector than CVE-2006-4783.	unknown 2006-10-18	7.0	CVE-2006-5388 OTHER-REF BID XF
WSN Forum -- WSN Forum	WSN Forum 1.3.4 and earlier allows remote attackers to execute arbitrary PHP code via a modified pathname in the pathtoconfig parameter that points to an avatar image that contains PHP code, which is then accessed from prestart.php. NOTE: this issue has been labeled remote file inclusion, but that label only applies to the attack, not the underlying vulnerability.	unknown 2006-10-20	7.0	CVE-2006-5421 OTHER-REF FRSIRT SECUNIA
XeoPort -- XeoPort	SQL injection vulnerability in index.php in XeoPort 0.81, and possibly earlier, allows remote attackers to execute arbitrary SQL commands via the xp_body_text parameter.	unknown 2006-10-13	7.0	CVE-2006-5285 FULLDISC BID BUGTRAQ

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info

Apache Software Foundation -- Apache	Format string vulnerability in the mod_tcl module 1.0 for Apache 2.x allows context-dependent attackers to execute arbitrary code via format string specifiers that are not properly handled in a set_var function call in (1) tcl_cmds.c and (2) tcl_core.c.	unknown 2006-10-16	5.6	CVE-2006-4154 IDEFENSE FRSIRT BID SECTRACK SECUNIA XF
BoonEx -- Dolphin	PHP remote file inclusion vulnerability in templates/tmpl_dfl/scripts/index.php in BoonEx Dolphin 5.2 allows remote attackers to execute arbitrary PHP code via a URL in the dir[inc] parameter. NOTE: it is possible that this issue overlaps CVE-2006-4189.	unknown 2006-10-20	5.6	CVE-2006-5410 BUGTRAQ BID XF
Cuttlefish Multimedia Ltd. -- Leicestershire communityPortals	PHP remote file inclusion vulnerability in includes/import-archive.php in Leicestershire communityPortals 1.0 build 20051018 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the cp_root_path parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-10-13	5.6	CVE-2006-5280 BID FRSIRT SECUNIA
CyberBrau -- CyberBrau	PHP remote file inclusion vulnerability in forum/track.php in CyberBrau 0.9.4, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the path parameter.	unknown 2006-10-18	5.6	CVE-2006-5400 OTHER-REF BID XF
db-central -- CMS db-central -- Enterprise CMS	Cross-site scripting (XSS) vulnerability in the search functionality in db-central (dbc) Enterprise CMS and db-central CMS allows remote attackers to inject arbitrary web script or HTML via the needle parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-10-20	4.7	CVE-2006-5430 BID SECUNIA

F5 -- FirePass 1000 SSL VPN	Cross-site scripting (XSS) vulnerability in my.acctab.php3 in F5 Networks FirePass 1000 SSL VPN 5.5, and possibly earlier, allows remote attackers to inject arbitrary web script or HTML via the sid parameter.	unknown 2006-10-20	5.6	CVE-2006-5416 BUGTRAQ OTHER-REF BID SECTRAK SECUNIA
Hastymail -- Hastymail	Hastymail 1.5 and earlier before 20061008 allows remote authenticated users to send arbitrary SMTP commands by placing them after a CRLF.CRLF sequence in the smtp_message parameter. NOTE: this crosses privilege boundaries if the SMTP server configuration prevents a user from establishing a direct SMTP session.	unknown 2006-10-17	4.2	CVE-2006-5313 OTHER-REF BID FRSIRT SECUNIA XF
Highwall -- Highwall Endpoint Highwall -- Highwall Enterprise	Multiple cross-site scripting (XSS) vulnerabilities in the wireless IDS management interface for Highwall Enterprise and Highwall Endpoint 4.0.2.11045 allow remote attackers to inject arbitrary HTML or web script via unspecified vectors.	unknown 2006-10-20	5.6	CVE-2006-5408 BUGTRAQ BID
HP -- Version Control Agent	Unspecified vulnerability in HP Version Control Agent before 2.1.5 allows remote authenticated users to obtain "unauthorized access" to a remote Repository Manager account and potentially gain privileges via unspecified vectors.	unknown 2006-10-17	4.2	CVE-2006-5300 HP BID FRSIRT SECTRAK SECUNIA XF
	Unspecified vulnerability in IBM WebSphere			CVE-2006-5323 OTHER-REF

IBM -- Websphere Application Server	Application Server before 6.1.0.2 has unspecified impact and attack vectors, related to a "possible security exposure," aka PK29360.	unknown 2006-10-17	4.9	OTHER-REF AIXAPAR FRSIRT SECUNIA
Justsystem -- Ichitaro	Unspecified vulnerability in Justsystem Ichitaro 2006, 2006 trial version, and Government 2006 allows remote attackers to execute arbitrary code via a modified document, possibly because of a buffer overflow, a different vulnerability than CVE-2006-4326.	unknown 2006-10-20	4.7	CVE-2006-5424 OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Microsoft -- PowerPoint	Buffer overflow in Microsoft Office 2003 PowerPoint allows user-assisted attackers to execute arbitrary code via a crafted PowerPoint (.PPT) file, as demonstrated by Nanika.ppt, and a different vulnerability than CVE-2006-3435, CVE-2006-3876, CVE-2006-3877, and CVE-2006-4694.	unknown 2006-10-16	5.6	CVE-2006-5296 OTHER-REF BID FRSIRT SECTRACK SECUNIA XF OTHER-REF OTHER-REF
Opera Software -- Opera	Heap-based buffer overflow in Opera 9.0 and 9.01 allows remote attackers to execute arbitrary code via a long URL in a tag (long link address).	unknown 2006-10-17	5.6	CVE-2006-4819 IDEFENSE OTHER-REF
				CVE-2006-

Oracle -- Oracle9i Database Server Oracle -- Oracle10g Database Server	Unspecified vulnerability in xdb.dbms_xdbz in the XMLDB component for Oracle Database 9.2.0.6 and 10.1.0.4 has unknown impact and remote authenticated attack vectors, aka Vuln# DB01.	unknown 2006-10-17	4.2	5332 ORACLE BID FRSIRT
Oracle -- Oracle10g Database Server	Multiple unspecified vulnerabilities in Oracle Database 10.1.0.5 and 10.2.0.2 have unknown impact and remote authenticated attack vectors related to (1) Vuln# DB04 and sys.dbms_cdc_impdp in the (a) Change Data Capture (CDC) component; (2) Vuln# DB07, (3) DB08, and (4) DB16 in sys.dbms_cdc_isubscribe in CDC; and (5) mdsys.sdo_geor_int in the (b) Oracle Spatial component, aka DB12.	unknown 2006-10-17	4.2	CVE-2006-5335 ORACLE BID FRSIRT
Oracle -- Oracle9i Database Server Oracle -- Oracle10g Database Server	Multiple unspecified vulnerabilities in the Change Data Capture (CDC) component in Oracle Database 9.2.0.7, 10.1.0.5, and have unknown impact and remote authenticated attack vectors related to (1) sys.dbms_cdc_ipublish (Vuln# DB05) and (2) sys.dbms_cdc_isubscribe (DB06).	unknown 2006-10-17	4.2	CVE-2006-5336 ORACLE BID FRSIRT
Oracle -- Oracle9i Database Server Oracle -- Oracle10g Database Server	Unspecified vulnerability in the Core RDBMS component in Oracle Database 9.0.1.5, 9.2.0.7, 10.1.0.5, and 10.2.0.2 has unknown impact and remote authenticated attack vectors, aka Vuln# DB09.	unknown 2006-10-17	4.2	CVE-2006-5337 ORACLE BID FRSIRT
Oracle -- Oracle10g Database Server	Unspecified vulnerability in the Core RDBMS component in Oracle Database 10.1.0.5 and 10.2.0.0 has unknown impact and remote authenticated attack vectors related to sys.dbms_sqlltune, aka Vuln# DB10.	unknown 2006-10-17	4.2	CVE-2006-5338 OTHER-REF BID FRSIRT
Oracle -- Oracle9i Database Server	Unspecified vulnerability in Oracle Spatial component in Oracle Database 8.1.7.4, 9.0.1.5, 9.2.0.7, and			CVE-2006-5339

Oracle -- Oracle10g Database Server Oracle -- Oracle8i Database Server	10.1.0.4 has unknown impact and remote authenticated attack vectors related to mdsys.sdo_geom, aka Vuln# DB11.	unknown 2006-10-17	4.2	ORACLE BID FRSIRT
Oracle -- Oracle9i Database Server Oracle -- Oracle10g Database Server	Multiple unspecified vulnerabilities in XMLDB component in Oracle Database 9.2.0.7, 10.1.0.5, and 10.2.0.2 have unknown impact and remote authenticated attack vectors, aka (1) Vuln# DB14 and (2) DB15 related to xdb.dbms_xdbz.	unknown 2006-10-17	4.2	CVE-2006-5341 ORACLE BID FRSIRT
Oracle -- Oracle10g Database Server	Unspecified vulnerability in Database Scheduler component in Oracle Database 10.1.0.3 has unknown impact and remote authenticated attack vectors related to sys.dbms_scheduler, aka Vuln# DB19.	unknown 2006-10-17	4.2	CVE-2006-5343 ORACLE BID FRSIRT
Oracle -- Oracle10g Database Server Oracle -- Oracle Database Server	Multiple unspecified vulnerabilities in Oracle Spatial component in Oracle Database 8.1.7.4, 9.0.1.5, 9.2.0.7, and 10.1.0.4 have unknown impact and remote authenticated attack vectors related to (1) mdsys.sdo_3gl, aka Vuln# DB20, and (2) mdsys.sdo_cs, aka DB21.	unknown 2006-10-17	4.2	CVE-2006-5344 OTHER- REF BID FRSIRT
Oracle -- Oracle10g Database Server Oracle -- Oracle Database Server	Unspecified vulnerability in Oracle Spatial component in Oracle Database 9.0.1.5, 9.2.0.7, and 10.1.0.4 has unknown impact and remote authenticated attack vectors related to mdsys.sdo_geom, aka Vuln# DB22.	unknown 2006-10-17	4.2	CVE-2006-5345 OTHER- REF BID FRSIRT
Oracle -- Oracle E-Business Suite and Applications Oracle -- Oracle Collaboration Suite Oracle -- Oracle HTTP	Unspecified vulnerability in Oracle HTTP Server 9.2.0.7, as used in Oracle Collaboration Suite 9.0.4.2 and Oracle E-Business Suite and Applications 11.5.10CU2, has unknown impact and remote attack vectors related to htdigest, aka Vuln# OHS02.	unknown 2006-10-17	5.6	CVE-2006-5346 ORACLE BID FRSIRT

Server				
Oracle -- Oracle E-Business Suite and Applications Oracle -- Oracle HTTP Server	Unspecified vulnerability in Oracle HTTP Server 9.2.0.7 and Oracle E-Business Suite and Applications 11.5.10CU2 has unknown impact and local attack vectors, aka Vuln# OHS08.	unknown 2006-10-17	4.9	CVE-2006-5350 OTHER-REF BID FRSIRT
Oracle -- E-Business Suite	Multiple unspecified vulnerabilities in Oracle E-Business Suite 11.5.7 up to 11.5.10CU2 have unknown impact and remote authenticated attack vectors, aka Vuln# (1) APPS03 in Oracle Applications Framework, (2) APPS04 in Oracle Applications Technology Stack, and (3) APPS05 in Oracle Balanced Scorecard, (4) APPS09 in Oracle Scripting, and (5) APPS10 in Oracle Trading Community.	unknown 2006-10-17	4.2	CVE-2006-5367 OTHER-REF BID FRSIRT
Oracle -- E-Business Suite	Unspecified vulnerability in Oracle Email Center component in Oracle E-Business Suite 11.5.9 has unknown impact and remote authenticated attack vectors, aka Vuln# APPS07.	unknown 2006-10-17	4.2	CVE-2006-5371 OTHER-REF BID FRSIRT
Oracle -- E-Business Suite	Multiple unspecified vulnerabilities in Oracle E-Business Suite 11.5.10 up to 11.5.10CU2 have unknown impact and remote authenticated attack vectors, aka Vuln# (1) APPS11 for Oracle Universal Work Queue and (2) APPS12 for Oracle Application Object Library.	unknown 2006-10-17	4.2	CVE-2006-5372 OTHER-REF BID FRSIRT
Oracle -- E-Business Suite	Unspecified vulnerability in Oracle Install Base component in Oracle E-Business Suite 11.5.10CU1 has unknown impact and remote authenticated attack vectors, aka Vuln# APPS13.	unknown 2006-10-17	4.2	CVE-2006-5373 OTHER-REF BID

				FRSIRT
Oracle -- Oracle PeopleSoft Enterprise	Multiple unspecified vulnerabilities in PeopleTools component in Oracle PeopleSoft Enterprise 8.22 GA, 8.46 GA, 8.47 GA, 8.48 GA, 8.22.11, 8.46.15, 8.47.09, and 8.48.03 have unknown impact and remote authenticated attack vectors, aka Vuln# (1) PSE04, (2) PSE06, (3) PSE07, and (4) PSE08.	unknown 2006-10-17	4.2	CVE-2006-5376 OTHER-REF BID FRSIRT
Oracle -- Oracle PeopleSoft Enterprise	Unspecified vulnerability in PeopleSoft component in Oracle PeopleSoft Enterprise 8.80 GA, 8.90 GA, 8.8 Bundle 11, and 8.9 Bundle 4 has unknown impact and remote authenticated attack vectors, aka Vuln# PSE05.	unknown 2006-10-17	4.2	CVE-2006-5377 OTHER-REF BID FRSIRT
Oracle -- EnterpriseOne	Unspecified vulnerability in JD Edwards HTML Server in JD Edwards EnterpriseOne SP23_O2, 8.95.P1, and 8.96.D1 has unknown impact and remote authenticated attack vectors, aka Vuln# JDE01.	unknown 2006-10-17	4.2	CVE-2006-5378 OTHER-REF BID FRSIRT
Php AMX -- Php AMX	PHP remote file inclusion vulnerability in plugins/main.php in Php AMX 0.9.0, when register_globals is enabled or magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary PHP code via a URL in the plug_path parameter.	unknown 2006-10-20	4.7	CVE-2006-5427 OTHER-REF BID FRSIRT SECUNIA XF
PHP News Reader -- PHP News Reader	PHP remote file inclusion vulnerability in auth/phpbb.inc.php in Shen Cheng-Da PHP News Reader (aka pnews) 2.6.4 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the CFG[auth_phpbb_path] parameter.	unknown 2006-10-13	5.6	CVE-2006-5284 Milw0rm BID FRSIRT

				SECUNIA
PHP Outburst -- Easynews	admin.php in PHP Outburst Easynews 4.4.1 and earlier, when register_globals is enabled, allows remote attackers to bypass authentication, and gain the ability to execute arbitrary code, via the en_login_id parameter.	unknown 2006-10-20	5.6	CVE-2006-5412 OTHER-REF BID SECUNIA
phpBB -- SpamBlockerMOD	PHP remote file inclusion vulnerability in includes/antispam.php in the SpamBlockerMODv 1.0.2 and earlier module for phpBB allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	unknown 2006-10-17	5.6	CVE-2006-5301 BUGTRAQ Milw0rm BID FRSIRT SECUNIA XF
phpBB -- lat2cyr	PHP remote file inclusion vulnerability in lat2cyr.php in the lat2cyr 1.0.1 and earlier phpbb module allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	unknown 2006-10-17	5.6	CVE-2006-5305 BUGTRAQ Milw0rm BID SECUNIA XF
Symantec -- Norton Internet Security Symantec -- Norton System Works Symantec -- Norton Antivirus Symantec -- Automated Support Assistant	Stack-based buffer overflow in an ActiveX control used in Symantec Automated Support Assistant, as used in Norton AntiVirus, Internet Security, and System Works 2005 and 2006, allows user-assisted remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors.	unknown 2006-10-18	5.6	CVE-2006-5403 OTHER-REF BID FRSIRT SECTRACK SECTRACK SECTRACK SECTRACK SECUNIA

Toshiba -- Bluetooth wireless device driver	Unspecified vulnerability in Toshiba Bluetooth wireless device driver 3.x and 4 through 4.00.35, as used in multiple products, allows physically proximate attackers to cause a denial of service (crash), corrupt memory, and possibly execute arbitrary code via crafted Bluetooth packets.	unknown 2006-10-18	5.6	CVE-2006-5405 BUGTRAQ OTHER-REF FRSIRT SECUNIA
Xeobook -- Xeobook	Multiple SQL injection vulnerabilities in sign.php in Xeobook 0.93 allow remote attackers to execute arbitrary SQL commands via (1) the User-Agent HTTP header, or the (2) gb_entry_text, (3) gb_location, (4) gb_fullname, or (5) gb_sex parameters.	2006-10-12 2006-10-13	5.6	CVE-2006-5287 FULLDISC BID

[Back to top](#)

Low Vulnerabilities				
Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Adobe -- Flash Player	CRLF injection vulnerability in Adobe Flash Player plugin 9.0.16 for Windows, 7.0.63 for Linux, and earlier versions allows remote attackers to modify HTTP headers of client requests and conduct HTTP Request Splitting attacks via CRLF sequences in arguments to the ActionScript functions (1) XML.setRequestHeader and (2) XML.contentType. NOTE: the flexibility of the attack varies depending on the type of web browser being used.	unknown 2006-10-17	2.3	CVE-2006-5330 OTHER-REF BUGTRAQ
Barry Nauta -- BRIM	Barry Nauta BRIM before 1.2.1 allows remote authenticated users to read information from other users via a modified URL.	unknown 2006-10-20	2.3	CVE-2006-5414 OTHER-REF SECUNIA

CipherTrust -- IronMail	Directory traversal vulnerability in IronWebMail before 6.1.1 HotFix-17 allows remote attackers to read arbitrary files via a GET request to the IM_FILE identifier with double-url-encoded "../" sequences ("%252e%252e/").	unknown 2006-10-16	2.3	CVE-2006-5210 BUGTRAQ OTHER-REF SYMANTEC BID FRSIRT SECTRAK SECUNIA
Cisco -- Cisco Secure Desktop	Cisco Secure Desktop (CSD) does not require that the ClearPageFileAtShutdown (aka CCE-Winv2.0-407) registry value equals 1, which might allow local users to read certain memory pages that were written during another user's SSL VPN session.	unknown 2006-10-18	1.6	CVE-2006-5393 CISCO SECTRAK
Cisco -- Cisco Secure Desktop	The default configuration of Cisco Secure Desktop (CSD) has an unchecked "Disable printing" box in Secure Desktop Settings, which might allow local users to read data that was sent to a printer during another user's SSL VPN session.	unknown 2006-10-18	1.6	CVE-2006-5394 CISCO SECTRAK
Clam Anti-Virus -- ClamAV	Unspecified vulnerability in ClamAV before 0.88.5 allows remote attackers to cause a denial of service (scanning service crash) via a crafted Compressed HTML Help (CHM) file that causes ClamAV to "read an invalid memory location."	2006-09-28 2006-10-16	2.3	CVE-2006-5295 IDEFENSE BID FRSIRT SECUNIA
Contenido -- Contendio	Contenido CMS stores sensitive data under the web root with insufficient access control, which allows remote attackers to obtain database credentials and other information via a direct request to (1) db_mysql.inc, (2) db_mssql.inc, (3) db_mysqli.inc, (4) db_oci8.inc, (5) db_odbc.inc, (6) db_oracle.inc, (7) db_pgsql.inc, or (8) db_sybase.inc in the conlib/	unknown 2006-10-18	2.3	CVE-2006-5381 BUGTRAQ

	directory.			
Gcontact -- Gcontact	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Gcontact 0.6.5 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2006-10-17	2.3	CVE-2006-5299 BUGTRAQ OTHER-REF BID
Kerio -- Winroute Firewall	Kerio WinRoute Firewall 6.2.2 and earlier allows remote attackers to cause a denial of service (crash) via malformed DNS responses.	unknown 2006-10-20	2.3	CVE-2006-5420 OTHER-REF BID FRSIRT SECTRACK
Linux -- Linux kernel	Linux kernel does not properly save or restore EFLAGS during a context switch, or reset the flags when creating new threads, which allows local users to cause a denial of service (process crash), as demonstrated using a process that sets the Alignment Check flag (EFLAGS 0x40000), which triggers a SIGBUS in other processes that have an unaligned access.	unknown 2006-10-17	1.6	CVE-2006-5173 OTHER-REF
McAfee -- Personal Firewall Plus McAfee -- VirusScan McAfee -- Network Agent McAfee -- Internet Security Suite	McAfee Network Agent (mcnasvc.exe) 1.0.178.0, as used by multiple McAfee products possibly including Internet Security Suite, Personal Firewall Plus, and VirusScan, allows remote attackers to cause a denial of service (agent crash) via a long packet, possibly because of an invalid string position field value. NOTE: some of these details are obtained from third party information.	unknown 2006-10-20	2.3	CVE-2006-5417 BUGTRAQ OTHER-REF BID SECTRACK SECUNIA XF
				CVE-2006-

Morian -- Album Photo Sans Nom	Directory traversal vulnerability in getimg.php in Album Photo Sans Nom 1.6 allows remote attackers to read arbitrary files via the img parameter.	unknown 2006-10-17	2.3	5320 OTHER-REF OTHER-REF SECUNIA FRSIRT
Mutt -- Mutt	Race condition in the safe_open function in the Mutt mail client 1.5.12 and earlier, when creating temporary files in an NFS filesystem, allows local users to overwrite arbitrary files due to limitations of the use of the O_EXCL flag on NFS filesystems.	unknown 2006-10-16	1.3	CVE-2006-5297 MLIST
Mutt -- Mutt	The mutt_adv_mktemp function in the Mutt mail client 1.5.12 and earlier does not properly verify that temporary files have been created with restricted permissions, which might allow local users to create files with weak permissions via a race condition between the mktemp and safe_fopen function calls.	unknown 2006-10-16	1.3	CVE-2006-5298 MLIST
Novell -- Bordermanager	Unspecified vulnerability in IKE.NLM in Novell BorderManager 3.8 allows attackers to cause a denial of service (crash) via unknown attack vectors related to "VPN issues" for certain "IKE and IPsec settings."	unknown 2006-10-13	2.3	CVE-2006-5286 OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
Oracle -- Oracle10g Database Server	Unspecified vulnerability in Oracle Spatial component in Oracle Database 10.2.0.2 has unknown impact and remote authenticated attack vectors related to "create session" and "create procedure" privileges, aka Vuln# DB02.	unknown 2006-10-17	3.4	CVE-2006-5333 ORACLE BID FRSIRT

Oracle -- Oracle9i Database Server Oracle -- Oracle10g Database Server	Unspecified vulnerability in Oracle Spatial component in Oracle Database 9.0.1.5, 9.2.0.7, and 10.1.0.5 has unknown impact and remote authenticated attack vectors related to mdsys.md2, aka Vuln# DB03.	unknown 2006-10-17	3.4	CVE-2006-5334 ORACLE BID FRSIRT
Oracle -- Oracle8i Database Server Oracle -- Oracle10g Database Server Oracle -- Oracle9i Database Server	Multiple unspecified vulnerabilities in Oracle Spatial component in Oracle Database 8.1.7.4, 9.0.1.5, 9.2.0.7, 10.1.0.5, and 10.2.0.2 have unknown impact and remote authenticated attack vectors related to (1) mdsys.sdo_lrs, aka Vuln# DB13, and (2) Vuln# DB17.	unknown 2006-10-17	3.4	CVE-2006-5340 ORACLE BID FRSIRT
Oracle -- Oracle9i Database Server Oracle -- Oracle10g Database Server	Unspecified vulnerability in Oracle Spatial component in Oracle Database 9.0.1.5, 9.2.0.6, and 10.1.0.3 has unknown impact and remote authenticated attack vectors related to mdsys.sdo_tune, aka Vuln# DB18.	unknown 2006-10-17	3.4	CVE-2006-5342 ORACLE BID FRSIRT
Passgo -- Defender	Passgo Defender 5.2 creates the application directory with insecure permissions (Everyone/Full Control), which allows local users to read and modify sensitive files. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-10-18	3.3	CVE-2006-5406 BID SECUNIA
PHPLibre -- RegistroTL	registroTL stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for /usuarios.dat.	unknown 2006-10-17	3.3	CVE-2006-5316 BUGTRAQ ACID- ROOT Milw0rm
Red Hat -- Red Hat Enterprise Linux	The kernel in Red Hat Enterprise Linux 3, when running on SMP systems, allows local users to cause a denial of service (deadlock) by running the shmat function on an shm at the same time that shmctl is	unknown 2006-10-17	1.9	CVE-2006-4342 REDHAT

	removing that shm (IPC_RMID), which prevents a spinlock from being unlocked.			
Secure Computing -- Safeword RemoteAccess	Secure Computing SafeWord RemoteAccess 2.1 allows local users to obtain the UserCenter webportal password, database encryption keys, and signing keys by reading (1) base-64 encoded data in SERVERS\Web\Tomcat\usercenter\WEB-INF\login.conf and (2) plaintext data in SERVERS\Shared\signers.cfg. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-10-17	1.6	CVE-2006-5303 BID SECUNIA XF
Sun -- Solaris	The tcp_fuse_rcv_drain function in the Sun Solaris 10 kernel before 20061017, when TCP Fusion is enabled, allows local users to cause a denial of service (system crash) via a TCP loopback connection with both endpoints on the same system.	unknown 2006-10-18	2.3	CVE-2006-5396 SUNALERT BID FRSIRT
Symantec -- Norton Internet Security Symantec -- Norton System Works Symantec -- Norton Antivirus Symantec -- Automated Support Assistant	Unspecified vulnerability in an ActiveX control used in Symantec Automated Support Assistant, as used in Norton AntiVirus, Internet Security, and System Works 2005 and 2006, allows user-assisted remote attackers to obtain sensitive information via unspecified vectors.	unknown 2006-10-18	1.9	CVE-2006-5404 OTHER-REF BID FRSIRT SECTRACK SECTRACK SECTRACK SECUNIA XF
				CVE-2006-5294 BUGTRAQ OTHER-REF

				XF
XORP -- eXtensible Open Router Platform	XORP (eXtensible Open Router Platform) 1.2 and 1.3 allows remote attackers to cause a denial of service (application crash) via an Open Shortest Path First (OSPF) Link State Advertisement (LSA) with an invalid LSA length field.	unknown 2006-10-20	2.3	CVE-2006-5425 FULLDISC OTHER-REF SECTRACK SECUNIA

[Back to top](#)

Last updated October 23, 2006