The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft -- Windows Internet Naming Service (WINS)	Windows Internet Naming Service (WINS) allows remote attackers to cause a denial of service (connectivity loss) or steal credentials via a 1Ch registration that causes WINS to change the domain controller to point to a malicious server. NOTE: this problem may be limited when Windows 95/98 clients are used, or if the primary domain controller becomes unavailable.	2009-01-14	7.6	CVE-1999-1593 MISC BID BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ NTBUGTRAQ
apple -- safari	Unspecified vulnerability in Apple Safari on Mac OS X 10.5 and Windows allows remote attackers to read arbitrary files on a client machine via vectors related to the association of Safari with the (1) feed, (2) feeds, and (3) feedsearch URL types for RSS feeds. NOTE: as of 20090114, the only disclosure is a vague pre-advisory. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.	2009-01-15	7.1	CVE-2009-0123 XF BID MISC MISC

codeavalanche -- freewallpaper	CodeAvalanche FreeWallpaper stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing the administrator password via a direct request for _private/CAFreeWallpaper.mdb. NOTE: some of these details are obtained from third party information.	2009-01-12	7.5	CVE-2008-5897 XF MILW0RM SECUNIA
devil -- developers_image_library	Multiple stack-based buffer overflows in the iGetHdrHeader function in src-IL/src/il_hdr.c in DevIL 1.7.4 allow context-dependent attackers to execute arbitrary code via a crafted Radiance RGBE file.	2009-01-13	7.5	CVE-2008-5262 BID MISC SECUNIA
google_cms -- google_cms	SQL injection vulnerability in frontpage.php in Goople CMS 1.8.2 allows remote attackers to execute arbitrary SQL commands via the password parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-01-14	7.5	CVE-2009-0121 SECUNIA
ibm -- websphere_datapower_xml_security_gateway_xs40	The IBM WebSphere DataPower XML Security Gateway XS40 with firmware 3.6.1.5 allows remote attackers to cause a denial of service (device reboot) by sending data over an established SSL connection, as demonstrated by the abc\r\n\r\n string data.	2009-01-14	7.8	CVE-2009-0120 BID BUGTRAQ
injader -- injader	SQL injection vulnerability in feeds.php in Injader before 2.1.2 allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: some of these details are obtained from third party information.	2009-01-12	7.5	CVE-2008-5890 BID
linux -- kernel	The sys_remap_file_pages function in mm/fremap.c in the Linux kernel before 2.6.24.1 allows local users to cause a denial of service or gain privileges via unspecified vectors, related to the vm_file structure member, and the mmap_region and do_munmap functions.	2009-01-13	7.2	CVE-2009-0024 BID
	Buffer overflow in SMB in the Server service in Microsoft			

microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via malformed values of unspecified "fields inside the SMB packets" in an NT Trans request, aka "SMB Buffer Overflow Remote Code Execution Vulnerability."	2009-01-14	10.0	CVE-2008-4834 MISC MS
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via malformed values of unspecified "fields inside the SMB packets" in an NT Trans2 request, related to "insufficiently validating the buffer size," aka "SMB Validation Remote Code Execution Vulnerability."	2009-01-14	10.0	CVE-2008-4835 MS
microsoft -- windows_xp	Buffer overflow in Microsoft Windows XP SP3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted .chm file.	2009-01-14	10.0	CVE-2009-0119 BID MILW0RM
microsoft -- html_help_workshop	Buffer overflow in Microsoft HTML Help Workshop 4.74 and earlier allows context-dependent attackers to execute arbitrary code via a .hhp file with a long "Index file" field, possibly a related issue to CVE-2006-0564.	2009-01-15	10.0	CVE-2009-0133 MILW0RM
oracle -- secure_backup	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.1.0.3 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2009-01-13	10.0	CVE-2008-4006 CONFIRM
oracle -- timesten_in-memory_database	Unspecified vulnerability in the TimesTen Data Server component in Oracle Database 7.0.5.0.0 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2009-01-13	7.5	CVE-2008-5440 CONFIRM
oracle -- secure_backup	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect	2009-01-13	10.0	CVE-2008-5444 CONFIRM

	confidentiality, integrity, and availability via unknown vectors.			CONFIRM
oracle -- secure_backup	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2009-01-13	10.0	CVE-2008-5448 CONFIRM
oracle -- secure_backup	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2009-01-13	10.0	CVE-2008-5449 CONFIRM
oracle -- bea_product_suite	Unspecified vulnerability in the Oracle BEA WebLogic Server Plugins for Apache, Sun and IIS web servers component in BEA Product Suite 10.3, 10.0, MP1, 9.2, MP3, 9.1, 9.0, 8.1, SP6, 7.0, and SP7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2009-01-13	10.0	CVE-2008-5457 CONFIRM
share2 -- easy_grid_control	Insecure method vulnerability in the EasyGrid.SGCtrl.32 ActiveX control in EasyGrid.ocx 1.0.0.1 in AAA EasyGrid ActiveX 3.51 allows remote attackers to create and overwrite arbitrary files via the (1) DoSaveFile or (2) DoSaveHtmlFile method. NOTE: vector 1 could be leveraged for code execution by creating executable files in Startup folders or by accessing files using hcp:// URLs. NOTE: some of these details are obtained from third party information.	2009-01-16	9.3	CVE-2009-0134 XF BID MILW0RM SECUNIA
suse -- opensuse	The web interface in git in SUSE openSUSE 10.3 allows remote attackers to execute arbitrary commands via shell metacharacters in an unspecified context.	2009-01-13	7.5	CVE-2008-5517 BID MISC MISC SUSE
xrdp -- xrdp	Buffer overflow in the xrdp_bitmap_invalidate function in xrdp/xrdp_bitmap.c in xrdp 0.4.1 and earlier allows remote attackers to execute arbitrary code via a crafted request.	2009-01-15	7.5	CVE-2008-5902 MISC MLIST
	Array index error in the			

xrdp -- xrdp	xrdp_bitmap_def_proc function in xrdp/funcs.c in xrdp 0.4.1 and earlier allows remote attackers to execute arbitrary code via vectors that manipulate the value of the edit_pos structure member.	2009-01-15	7.5	CVE-2008-5903 MISC MLIST
xrdp -- xrdp	The rdp_rdp_process_color_pointer_pdu function in rdp/rdp_rdp.c in xrdp 0.4.1 and earlier allows remote RDP servers to have an unknown impact via input data that sets crafted values for certain length variables, leading to a buffer overflow.	2009-01-15	7.5	CVE-2008-5904 MISC MLIST

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.1.0.1 allows remote attackers to affect confidentiality via unknown vectors.	2009-01-13	5.0	CVE-2008-3981 CONFIRM
arrl -- tqsllib	The tqsl_verifyDataBlock function in openssl_cert.cpp in American Radio Relay League (ARRL) tqsllib 2.0 does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	2009-01-15	5.0	CVE-2009-0124 CONFIRM MLIST MISC
asterisk -- asterisk_business_edition asterisk -- open_source asterisk -- s800i_appliance	IAX2 in Asterisk Open Source 1.2.x before 1.2.31, 1.4.x before 1.4.23-rc4, and 1.6.x before 1.6.0.3-rc2; Business Edition A.x.x, B.x.x before B.2.5.7, C.1.x.x before C.1.10.4, and C.2.x.x before C.2.1.2.1; and s800i 1.2.x before 1.3.0 responds differently to a failed login attempt depending on whether the user account exists, which allows remote attackers to enumerate valid usernames.	2009-01-14	5.0	CVE-2009-0041 BID
berkeley -- boinc_client	The decrypt_public function in lib/crypt.cpp in the client in Berkeley Open Infrastructure for Network Computing (BOINC) 6.2.14 and 6.4.5 does not check the return value from the OpenSSL RSA_public_decrypt	2009-01-	5.0	CVE-2009-0126 CONFIRM MLIST

berkeley -- boinc_client	the OpenSSL RSA_public_decrypt function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	15	5.0	MLIST CONFIRM CONFIRM CONFIRM
erlang -- erlang	** DISPUTED ** lib/crypto/c_src/crypto_drv.c in erlang does not properly check the return value from the OpenSSL DSA_do_verify function, which might allow remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077. NOTE: a package maintainer disputes this issue, reporting that there is a proper check within the only code that uses the applicable part of crypto_drv.c, and thus "this report is invalid."	2009-01-15	5.0	CVE-2009-0130 MLIST MISC
finkproject -- libnasl	nasl/nasl_crypto2.c in the Nessus Attack Scripting Language library (aka libnasl) 2.2.11 does not properly check the return value from the OpenSSL DSA_do_verify function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	2009-01-15	5.0	CVE-2009-0125 CONFIRM MLIST CONFIRM MISC
heikkitoivonen -- m2crypto	** DISPUTED ** M2Crypto does not properly check the return value from the OpenSSL EVP_VerifyFinal, DSA_verify, ECDSA_verify, DSA_do_verify, and ECDSA_do_verify functions, which might allow remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077. NOTE: a Linux vendor disputes the relevance of this report to the M2Crypto product because "these functions are not used anywhere in m2crypto."	2009-01-15	5.0	CVE-2009-0127 MISC MLIST MISC
hp -- hplip	hplip.postinst in HP Linux Imaging and Printing (HPLIP) 2.7.7 and 2.8.2 on Ubuntu allows local users to change the ownership of arbitrary files via unspecified manipulations in advance of an HPLIP installation or upgrade by an administrator, related to the product's attempt to correct the	2009-01-15	6.9	CVE-2009-0122 BID

	ownership of its configuration files within home directories.			
jdedwards -- enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the JD Edwards Tools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.97.2.5 allows remote authenticated users to affect confidentiality via unknown vectors.	2009-01-13	4.0	CVE-2008-5451 CONFIRM
jdedwards -- enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the PeopleSoft Enterprise HRMS component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.9.18 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2009-01-13	5.5	CVE-2008-5452 CONFIRM
jdedwards -- enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the PeopleSoft Enterprise HRMS - ePerformance component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.9.18 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2009-01-13	4.9	CVE-2008-5455 CONFIRM
ktorrent -- ktorrent	The web interface plugin in KTorrent before 3.1.4 allows remote attackers to bypass intended access restrictions and upload arbitrary torrent files, and trigger the start of downloads and seeding, via a crafted HTTP POST request.	2009-01-15	4.3	CVE-2008-5905 CONFIRM SECUNIA SECUNIA MLIST CONFIRM CONFIRM
ktorrent -- ktorrent	Eval injection vulnerability in the web interface plugin in KTorrent before 3.1.4 allows remote attackers to execute arbitrary PHP code via unspecified parameters to this interface's PHP scripts.	2009-01-15	6.8	CVE-2008-5906 CONFIRM SECUNIA SECUNIA MLIST CONFIRM CONFIRM
libpng -- libpng	The png_check_keyword function in pngwutil.c in libpng before 1.0.42, and 1.2.x before 1.2.34, might allow context-dependent attackers to set the value of an arbitrary memory location to zero via vectors involving creation of crafted PNG files with keywords, related to an implicit cast of the '\0' character constant to a NULL pointer. NOTE: some sources incorrectly report this as a double free vulnerability.	2009-01-15	5.0	CVE-2008-5907 MLIST MLIST CONFIRM

linux -- kernel	Race condition in the do_setlk function in fs/nfs/file.c in the Linux kernel before 2.6.26 allows local users to cause a denial of service (crash) via vectors resulting in an interrupted RPC call that leads to a stray FL_POSIX lock, related to improper handling of a race between fcntl and close in the EINTR case.	2009-01-13	4.0	CVE-2008-4307 CONFIRM CONFIRM MLIST CONFIRM
linux -- kernel	The ABI in the Linux kernel 2.6.28 and earlier on s390, powerpc, sparc64, and mips 64-bit platforms requires that a 32-bit argument in a 64-bit register was properly sign extended when sent from a user-mode application, but cannot verify this, which allows local users to cause a denial of service (crash) or possibly gain privileges via a crafted system call.	2009-01-15	4.6	CVE-2009-0029 CONFIRM BID SECUNIA MLIST
llnl -- slurm	plugins/crypto/openssl/crypto_openssl.c in Simple Linux Utility for Resource Management (aka SLURM or slurm-llnl) does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	2009-01-15	5.0	CVE-2009-0128 MLIST MISC
microsoft -- internet_information_services	Microsoft Internet Information Services (IIS) 5.0 does not log requests that use the TRACK method, which allows remote attackers to obtain sensitive information without detection.	2009-01-14	5.0	CVE-2003-1566 XF BID OSVDB MISC NTBUGTRAQ
microsoft -- internet_information_services	The undocumented TRACK method in Microsoft Internet Information Services (IIS) 5.0 returns the content of the original request in the body of the response, which makes it easier for remote attackers to steal cookies and authentication credentials, or bypass the HttpOnly protection mechanism, by using TRACK to read the contents of the HTTP headers that are returned in the response, a technique that is similar to cross-site tracing (XST) using HTTP TRACE.	2009-01-14	5.8	CVE-2003-1567 CERT-VN OSVDB MISC NTBUGTRAQ
	Unspecified vulnerability in the Oracle OLAP component in Oracle Database			CVE-2008

oracle -- database_9i	9.0.2.8 and 9.2.0.8DV allows remote authenticated users to affect availability, related to SYS.OLAPIMPL_T.	2009-01-13	4.0	CVE-2008-3974 CONFIRM
oracle -- database_10g	Unspecified vulnerability in the Oracle Spatial component in Oracle Database 10.1.0.5 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2009-01-13	5.5	CVE-2008-3978 CONFIRM
oracle -- database_10g	Unspecified vulnerability in the Oracle Spatial component in Oracle Database 10.1.0.5 and 10.2.0.2 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2009-01-13	5.5	CVE-2008-3979 CONFIRM
oracle -- database_10g	Unspecified vulnerability in the Oracle OLAP component in Oracle Database 10.1.0.5 and 10.2.0.3 allows remote authenticated users to affect availability, related to SYS.DBMS_XSOQ_ODBO.	2009-01-13	4.0	CVE-2008-3997 CONFIRM
oracle -- database_10g oracle -- database_9i	Unspecified vulnerability in the Oracle OLAP component in Oracle Database 9.2.0.8, 9.2.0.8DV, and 10.1.0.5 allows remote authenticated users to affect availability, related to SYS.OLAPIMPL_T.	2009-01-13	4.0	CVE-2008-3999 CONFIRM
oracle -- database_10g	Unspecified vulnerability in the Oracle Streams component in Oracle Database 10.1.0.5 allows remote authenticated users to affect confidentiality and integrity, related to SYS.DBMS_STREAMS_AUTH.	2009-01-13	5.5	CVE-2008-4015 CONFIRM
oracle -- database_10g oracle -- database_9i	Unspecified vulnerability in the Oracle OLAP component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.4 allows remote authenticated users to affect integrity and availability via unknown vectors.	2009-01-13	5.5	CVE-2008-5436 CONFIRM
oracle -- database_10g oracle -- database_11i oracle -- database_9i	Unspecified vulnerability in the Job Queue component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity, related to DBMS_IJOB.	2009-01-13	5.5	CVE-2008-5437 CONFIRM
oracle -- database_10g	Unspecified vulnerability in the SQL*Plus Windows GUI component in Oracle Database 10.2.0.4 allows remote authenticated users to affect confidentiality via unknown vectors.	2009-01-13	4.0	CVE-2008-5439 CONFIRM

oracle -- secure_backup	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect availability via unknown vectors.	2009-01-13	5.0	CVE-2008-5441 CONFIRM
oracle -- secure_backup	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect availability via unknown vectors.	2009-01-13	5.0	CVE-2008-5442 CONFIRM
oracle -- jd_edwards_enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the PeopleSoft Enterprise Components component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.9.18 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.	2009-01-13	6.5	CVE-2008-4007 CONFIRM
oracle -- application_server	Unspecified vulnerability in the Oracle BPEL Process Manager component in Oracle Application Server None allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2009-01-13	5.5	CVE-2008-4014 CONFIRM
oracle -- collaboration_suite	Unspecified vulnerability in the Collaborative Workspaces component in Oracle Collaboration Suite 10.1.2 allows remote authenticated users to affect confidentiality via unknown vectors.	2009-01-13	4.0	CVE-2008-4016 CONFIRM
oracle -- application_server	Unspecified vulnerability in the OC4J component in Oracle Application Server 10.1.2.3 allows remote attackers to affect confidentiality via unknown vectors.	2009-01-13	5.0	CVE-2008-4017 CONFIRM
oracle -- application_server_10g	Unspecified vulnerability in the Oracle Portal component in Oracle Application Server 10.1.2.3 and 10.1.4.2 allows remote attackers to affect integrity via unknown vectors.	2009-01-13	4.3	CVE-2008-5438 CONFIRM
oracle -- secure_backup	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect availability via unknown vectors.	2009-01-13	5.0	CVE-2008-5443 CONFIRM
oracle -- secure_backup	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.2 allows remote attackers to affect availability via unknown vectors.	2009-01-13	5.0	CVE-2008-5445 CONFIRM
	Unspecified vulnerability in the Oracle			

oracle -- enterprise_manager_grid_control_10g	Enterprise Manager component in Oracle Enterprise Manager 10.2.0.4 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2009-01-13	5.5	CVE-2008-5447 CONFIRM
oracle -- e-business_suite_11i oracle -- e-business_suite_12	Unspecified vulnerability in the iProcurement component in Oracle E-Business Suite 11.5.10, CU2, and 12.0.6 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2009-01-13	4.9	CVE-2008-5454 CONFIRM
oracle -- jd_edwards_enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the PeopleSoft Enterprise HRMS component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.9.18 and 9.0.8 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2009-01-13	4.9	CVE-2008-5456 CONFIRM
oracle -- e-business_suite oracle -- e-business_suite_12	Unspecified vulnerability in the Oracle Application Object Library component in Oracle E-Business Suite 11.5.10 and CU2 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2009-01-13	5.5	CVE-2008-5458 CONFIRM
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.3 allows remote attackers to affect confidentiality via unknown vectors.	2009-01-13	5.0	CVE-2008-5459 CONFIRM
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.3, 10.0, MP1, 9.2, MP3, 9.1, 9.0, 8.1, SP6, 7.0, and SP7 allows remote attackers to affect confidentiality, integrity, and availability, related to WLS.	2009-01-13	6.8	CVE-2008-5461 CONFIRM
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Portal component in BEA Product Suite 10.3, 10.2, 10.0, MP1, 9.2, MP3, 8.1, and SP6 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2009-01-13	6.8	CVE-2008-5462 CONFIRM
oracle -- jd_edwards_enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the PeopleSoft Enterprise Campus Solutions component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.9.18 and 9.0.8 allows remote authenticated users to affect confidentiality and integrity via	2009-01-13	4.9	CVE-2008-5463 CONFIRM

	unknown vectors.			
perl-openssl -- libcrypt-openssl-dsa-perl	libcrypt-openssl-dsa-perl does not properly check the return value from the OpenSSL DSA_verify and DSA_do_verify functions, which might allow remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	2009-01-15	5.0	CVE-2009-0129 MLIST CONFIRM
phplist -- phplist	phplist before 2.10.8 allows remote attackers to include files via unknown vectors, related to a "local file include vulnerability."	2009-01-12	5.0	CVE-2008-5887 BID BUGTRAQ CONFIRM SECUNIA
sun -- opensolaris	The UFS implementation in the kernel in Sun OpenSolaris snv_29 through snv_90 allows local users to cause a denial of service (panic) via the single posix_fallocate test in the SUSv3 POSIX test suite, related to an F_ALLOCSP fcntl call.	2009-01-15	4.9	CVE-2009-0131 BID SUNALERT CONFIRM
sun -- opensolaris sun -- solaris	Integer overflow in the aio_suspend function in Sun Solaris 8 through 10 and OpenSolaris, when 32-bit mode is enabled, allows local users to cause a denial of service (panic) via a large integer value in the second argument (aka nent argument).	2009-01-15	4.9	CVE-2009-0132 BID CONFIRM
takempis -- discussion_web	TAKempis Discussion Web 4.0 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing a password via a direct request for _private/discussion.mdb. NOTE: some of these details are obtained from third party information.	2009-01-12	5.0	CVE-2008-5886 XF MILW0RM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- database_10g oracle -- database_11g	Unspecified vulnerability in the SQL*Plus Windows GUI component in Oracle Database allows local users to affect confidentiality via unknown vectors.	2009-01-13	1.7	CVE-2008-3973 CONFIRM
oracle -- jdeveloper	Unspecified vulnerability in the Oracle JDeveloper component in Oracle Application Server 10.1.2.3 allows local users to affect confidentiality via	2009-01-13	2.1	CVE-2008-2623 CONFIRM

	unknown vectors.			CONFIRM
oracle -- e-business_suite oracle -- e-business_suite_12	Unspecified vulnerability in the Oracle Applications Framework component in Oracle E-Business Suite 11.5.10, CU2, and 12.0.6 allows remote authenticated users to affect confidentiality via unknown vectors.	2009-01-13	3.5	CVE-2008-5446 CONFIRM
oracle -- e-business_suite oracle -- e-business_suite_12	Unspecified vulnerability in the Oracle Applications Platform Engineering component in Oracle E-Business Suite 11.5.10, CU2, and 12.0.6 allows local users to affect confidentiality via unknown vectors.	2009-01-13	1.2	CVE-2008-5450 CONFIRM
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.3, 10.0, MP1, 9.2, MP3, 9.1, and 9.0 allows remote attackers to affect confidentiality via unknown vectors.	2009-01-13	2.6	CVE-2008-5460 CONFIRM
Back to top				