

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 (NCSA) / 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
acresso -- flexnet_connect	Insecure method vulnerability in the MVSNCClientWebAgent61.WebAgent.1 ActiveX control (isusweb.dll 6.1.100.61372) in Macrovision FLEXnet Connect 6.1 allows remote attackers to force the download and execution of arbitrary files via the DownloadAndExecute method.
acresso -- flexnet_connect	Insecure method vulnerability in the MSVNClientDownloadManager61Lib.DownloadManager ActiveX control (ISDM.exe 6.1.100.61372) in Macrovision FLEXnet Connect 6.1 allows remote attackers to force the download and execution of arbitrary files via the AddFile and RunScheduledJobs methods. NOTE: this could be leveraged for code execution by uploading executable files to Startup folders.
apple -- cups	The Hewlett-Packard Graphics Language (HPGL) filter in CUPS before 1.3.9 allows remote attackers to execute arbitrary code via crafted pen width and pen color opcodes that overwrite arbitrary memory.
apple -- cups	Heap-based buffer overflow in the read_rle16 function in imagetops in CUPS before 1.3.9 allows remote attackers to execute arbitrary code via an SGI image with malformed Run Length Encoded (RLE) data containing a small image and a large row count.
Back to top	

High Vulnerabilities	
Primary Vendor -- Product	Description
aspindir -- munzursoft_web_portal_w3	SQL injection vulnerability in kategori.asp in MunzurSoft Wep Portal W3 allows remote attackers to execute arbitrary SQL commands via the kat parameter.
aspindir -- ayco_okul_portali	SQL injection vulnerability in default.asp in Ayco Okul Portali allows remote attackers to execute arbitrary SQL commands via the linkid parameter.
belong_software -- site_builder	Belong Software Site Builder 0.1 beta allows remote attackers to bypass intended access restrictions and perform administrative actions via a direct request to admin/home.php.
ca -- arcserve_backup ca -- business_protection_suite ca -- server_protection_suite	Directory traversal vulnerability in the RPC interface (asdbapi.dll) in CA ARCserve Backup (formerly BrightStor ARCserve Backup) r11.1 through r12.0 allows remote attackers to execute arbitrary commands via a .. (dot dot) in an RPC call with opnum 0x10A.
chilkat_software -- ftp	Insecure method vulnerability in the Chilkat FTP 2.0 ActiveX component (ChilkatCert.dll) allows remote attackers to overwrite arbitrary files via a full pathname in the SavePkcs8File method.
cisco -- unity	Cisco Unity 4.x before 4.2(1)ES161, 5.x before 5.0(1)ES5 and 7.x before 7.0(2)ES8, when using anonymous authentication (aka native Unity authentication), allows remote attackers to cause a denial of service (session exhaustion) via a large number of connections.
cutephp -- cutenews	plugins/wacko/highlight/html.php in Strawberry in CuteNews.ru 1.1.1 (aka Strawberry) allows remote attackers to execute arbitrary PHP code via the text parameter, which is inserted into an executable regular expression.
dvrhost -- web_cms	Heap-based buffer overflow in the PdvrAtl.PdvrOcx.1 ActiveX control (pdvratl.dll) in DVRHOST Web CMS OCX 1.0.1.25 allows remote attackers to execute arbitrary code via a long second argument to the TimeSpanFormat method.

[Back to top](#)

High Vulnerabilities	
Primary Vendor -- Product	Description
etype -- eserv	Stack-based buffer overflow in the FTP server in Etype Eserv 3.x, possibly 3.26, allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via a long argument to the ABOR command
gentoo -- cman gentoo -- fence	fence_manual in fence allows local users to modify arbitrary files via a symlink attack on the fence_manual.fif temporary file.
graphviz -- graphviz	Stack-based buffer overflow in the push_subg function in parser.y (lib/graph/parser.c) in Graphviz 2.20.2, and possibly earlier versions, allows user-assisted remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a DOT file with a large number of Agraph_t elements.
guildftpd -- guildftpd	GuildFTPD 0.999.14, and possibly other versions, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via long arguments to the CWD and LIST commands, which triggers heap corruption related to an improper free call, and possibly triggering a heap-based buffer overflow.
hp -- openview_network_node_manager	Multiple stack-based buffer overflows in ovalarmsrv in HP OpenView Network Node Manager (OV NNM) 7.51, and possibly 7.01, 7.50, and 7.53, allow remote attackers to execute arbitrary code via a long (1) REQUEST_SEV_CHANGE (aka number 47), (2) REQUEST_SAVE_STATE (aka number 61), or (3) REQUEST_RESTORE_STATE (aka number 62) request to TCP port 2954.
hp -- openview_network_node_manager	Unspecified vulnerability in ovtopmd in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to cause a denial of service via unknown vectors, a different vulnerability than CVE-2008-3536, CVE-2008-3537, and CVE-2008-3544. NOTE: due to insufficient details from the vendor, it is not clear whether this is the same as CVE-2008-1853.
lenovo -- resuce_and_recovery	Heap-based buffer overflow in the tvtumin.sys kernel driver in Lenovo Rescue and Recovery 4.20, including 4.20.0511 and 4.20.0512, allows local users to execute arbitrary code via a long file name.
linksys -- wap400n	The Marvell driver for the Linksys WAP4400N Wi-Fi access point with firmware 1.2.14 on the Marvell 88W8361P-BEM1 chipset, when WEP mode is enabled, does not properly parse malformed 802.11 frames, which allows remote attackers to cause a denial of service (reboot or hang-up) via a malformed association request containin

[Back to top](#)

High Vulnerabilities	
Primary Vendor -- Product	Description
	the WEP flag, as demonstrated by a request that is too short, is a different vulnerability than CVE-2008-1144 and CVE-2008-1197.
linux -- kernel	sctp in Linux kernel before 2.6.25.18 allows remote attackers to cause a denial of service (OOPS) via an INIT-ACK that states the peer does not support AUTH, which causes the sctp_process_init function to clean up active transports and triggers the OOPS when the T1-Init timer expires.
microsoft -- host_integration_server	Microsoft Host Integration Server (HIS) 2000, 2004, and 2006 does not limit RPC access to administrative functions, which allows remote attackers to bypass authentication and execute arbitrary code via a crafted SNA RPC message, aka "HIS Command Execution Vulnerability."
microsoft -- open_xml_file_format_converter microsoft -- office microsoft -- office_compatibility_pack_for_word_excel_ppt_2007 microsoft -- office_excel_viewer microsoft -- office_sharepoint_server	Microsoft Excel 2000 SP3, 2002 SP3, 2003 SP2 and SP3, and 2007 Gold and SP1; Office Excel Viewer 2003 SP3; Office Excel Viewer; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; Office 2004 and 2008 for Mac; and Open XML File Format Converter for Mac do not properly allocate memory when loading Excel objects during parsing of the Excel spreadsheet file format, which allows remote attackers to execute arbitrary code via a crafted BIFF file, aka "File Format Parsing Vulnerability."
microsoft -- open_xml_file_format_converter microsoft -- office microsoft -- office_compatibility_pack_for_word_excel_ppt_2007 microsoft -- office_excel_viewer microsoft -- office_sharepoint_server	Integer overflow in the REPT function in Microsoft Excel 2000 SP3, 2002 SP3, 2003 SP2 and SP3, and 2007 Gold and SP1; Office Excel Viewer 2003 SP3; Office Excel Viewer; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; Office SharePoint Server 2007 Gold and SP1; Office 2004 and 2008 for Mac; and Open XML File Format Converter for Mac allows remote attackers to execute arbitrary code via an Excel file containing a formula within a cell, aka "Formula Parsing Vulnerability."
microsoft -- iis microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_xp	Integer overflow in the Internet Printing Protocol (IPP) ISAPI extension in Microsoft Internet Information Service (IIS) 5.0 through 7.0 on Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to execute arbitrary code via an HTTP POST request that triggers an outbound IPP connection from a web server to a machine operated by the attacker, aka "Integer Overflow in IPP Service Vulnerability."
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008	The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate window properties

High Vulnerabilities	
Primary Vendor -- Product	Description
microsoft -- windows_vista microsoft -- windows_xp	sent from a parent window to a child window during creation of a new window, which allows local users to gain privileges via a crafted application, aka "Windows Kernel Window Creation Vulnerability."
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_xp	Double free vulnerability in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 ar SP2, Vista Gold and SP1, and Server 2008 allows local users to gain privileges via a crafted application that make: system calls within multiple threads, aka "Windows Kerne Unhandled Exception Vulnerability." NOTE: according to Microsoft, this is not a duplicate of CVE-2008-4510.
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate parameters sent from user mode to the kernel, which allows local users to gain privileges via a crafted application, aka "Windows Kernel Memory Corruption Vulnerability."
microsoft -- windows_2003_server microsoft -- windows_xp	afd.sys in the Ancillary Function Driver (AFD) component in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP1 and SP2 does not properly validate input sent from user mode to the kernel, which allows local user to gain privileges via a crafted application, aka "AFD Kernel Overwrite Vulnerability."
microsoft -- internet_explorer	Microsoft Internet Explorer 6 and 7 does not properly determine the domain or security zone of origin of web script, which allows remote attackers to bypass the intende cross-domain security policy, and execute arbitrary code o obtain sensitive information, via a crafted HTML documer aka "HTML Element Cross-Domain Vulnerability."
microsoft -- internet_explorer	Microsoft Internet Explorer 6 and 7 does not properly determine the domain or security zone of origin of web script, which allows remote attackers to bypass the intende cross-domain security policy, and execute arbitrary code o obtain sensitive information, via a crafted HTML documer aka "Event Handling Cross-Domain Vulnerability."
microsoft -- internet_explorer	Microsoft Internet Explorer 6 does not properly handle errors associated with access to an object that has been (1) incorrectly initialized or (2) deleted, which allows remote attackers to execute arbitrary code via a crafted HTML document, aka "Uninitialized Memory Corruption Vulnerability."
microsoft -- internet_explorer	Microsoft Internet Explorer 5.01 SP4 and 6 does not properly handle errors associated with access to uninitialized memory, which allows remote attackers to execute arbitrary code via a crafted HTML document, aka

[Back to top](#)

High Vulnerabilities	
Primary Vendor -- Product	Description
	"HTML Objects Memory Corruption Vulnerability."
microsoft -- internet_explorer	Microsoft Excel 2000 SP3, 2002 SP3, and 2003 SP2 and SP3 does not properly validate data in the VBA Performance Cache, which allows remote attackers to execute arbitrary code via a crafted Excel file, aka "Calendar Object Validation Vulnerability."
microsoft -- windows_2000	The Microsoft Message Queuing (MSMQ) service in Microsoft Windows 2000 SP4 does not properly validate parameters to string APIs, which allows remote attackers to execute arbitrary code via a crafted RPC call that overflow a "heap request," aka "Message Queuing Service Remote Code Execution Vulnerability."
microsoft -- windows_2000	Active Directory in Microsoft Windows 2000 SP4 does not properly allocate memory for (1) LDAP and (2) LDAPS requests, which allows remote attackers to execute arbitrary code via a crafted request, aka "Active Directory Overflow Vulnerability."
microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Integer overflow in Memory Manager in Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vis Gold and SP1, and Server 2008 allows local users to gain privileges via a crafted application that triggers an erroneous decrement of a variable, related to validation of parameters for Virtual Address Descriptors (VADs) and a "memory allocation mapping error," aka "Virtual Address Descriptor Elevation of Privilege Vulnerability."
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Buffer underflow in Microsoft Windows 2000 SP4, XP SP and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via a Server Message Block (SMB) request that contains a filename with a crafted length, aka "SMB Buffer Underflow Vulnerability."
nfs -- nfs-utils	nfs-utils 1.0.9, and possibly other versions before 1.1.3, invokes the host_ctl function with the wrong order of arguments, which causes TCP Wrappers to ignore netgroup and allows remote attackers to bypass intended access restrictions.
novell -- edirectory	Multiple integer overflows in dhost.exe in Novell eDirectory 8.8 before 8.8.3, and 8.7.3 before 8.7.3.10 ftf1, allow remote attackers to execute arbitrary code via a crafted (1) Content-Length header in a SOAP request or (2) Netware Core Protocol opcode 0x0F message, which triggers a heap-based buffer overflow.
novell -- edirectory	Heap-based buffer overflow in dhost.exe in Novell eDirectory 8.8 before 8.8.3, and 8.7.3 before 8.7.3.10 ftf1, allows remote attackers to execute arbitrary code via a

[Back to top](#)

High Vulnerabilities	
Primary Vendor -- Product	Description
	SOAP request with a long Accept-Language header.
novell -- edirectory	Heap-based buffer overflow in dhost.exe in Novell eDirectory 8.x before 8.8.3, and 8.7.3 before 8.7.3.10 ftf1, allows remote attackers to execute arbitrary code via a crafted Netware Core Protocol opcode 0x24 message that triggers a calculation error that under-allocates a heap buffer.
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server Plugins for Apache component in BEA Product Suite 10.3, 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, 7.0 SP7, and 6.1 SP7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.
qemu -- qemu	qemu-make-debian-root in qemu 0.9.1-5 on Debian GNU/Linux allows local users to overwrite arbitrary files via a symlink attack on temporary files and directories.
real-estate-scripts -- real-estate-scripts	SQL injection vulnerability in index.php in Real Estate Classifieds allows remote attackers to execute arbitrary SQL commands via the cat parameter.
rtssentry -- rtssentry	Stack-based buffer overflow in the PTZCamPanelCtrl ActiveX control (CamPanel.dll) in RTS Sentry 2.1.0.2 allows remote attackers to execute arbitrary code via a long second argument to the ConnectServer method.
sportspanel -- sports_clubs_web_portal	Directory traversal vulnerability in index.php in Sports Clubs Web Panel 0.0.1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the p parameter.
stash -- stash	Multiple SQL injection vulnerabilities in Stash 1.0.3 allow remote attackers to execute arbitrary SQL commands via (1) the username parameter to admin/login.php and (2) the pos parameter to admin/news.php.
sun -- java_system_web_proxy_server	Heap-based buffer overflow in the FTP subsystem in Sun Java System Web Proxy Server 4.0 through 4.0.7 allows remote attackers to execute arbitrary code via unspecified vectors.
sun -- solaris	Stack-based buffer overflow in the adm_build_path function in sadmind in Sun Solstice AdminSuite on Solaris 8 and 9 allows remote attackers to execute arbitrary code via a crafted request.

[Back to top](#)

High Vulnerabilities	
Primary Vendor -- Product	Description
systemrequirementslab -- system_requirements_lab	Husdawg, LLC Systems Requirements Lab 3 allows remote attackers to force the download and execution of arbitrary programs via unknown vectors in (1) ActiveX control (sysreqlab.dll, sysreqlabli.dll, or sysreqlab2.dll) and (2) Java applet in RLApplet.class in sysreqlab2.jar or sysreqlab.jar.
xigla -- absolute_poll_manager_xe	SQL injection vulnerability in xlacomments.asp in XIGLA Software Absolute Poll Manager XE 4.1 allows remote attackers to execute arbitrary SQL commands via the p parameter.

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- flash_player	Adobe Flash Player 9.0.45.0, 9.0.112.0, 9.0.124.0, and 10.0.12.10 allows remote web servers to cause a denial of service (NULL pointer dereference and browser crash) by returning a different response when an HTTP request is sent a second time, as demonstrated by two responses that provide SWF files with different SWF version numbers.	2008-10-14	4.3	CVE-2008-4546 BUGTRAQ MISC
adobe -- flash_player	ActionScript in Adobe Flash Player 9.0.124.0 and earlier does not require user interaction in conjunction with (1) the FileReference.browse operation in the FileReference upload API or (2) the FileReference.download operation in the FileReference download API, which allows remote attackers to create a browse dialog box, and possibly have unspecified other impact, via an SWF file.	2008-10-17	5.0	CVE-2008-4401 XF CONFIRM SECUNIA
apache -- tomcat	Apache Tomcat 5.5.0 and 4.1.0 through 4.1.31 allows remote attackers to bypass an IP address restriction and obtain sensitive information via a request that is processed concurrently with another request but in a different thread, leading to an instance-variable overwrite associated with a "synchronization problem" and lack of thread safety, and related to RemoteFilterValve, RemoteAddrValve, and RemoteHostValve.	2008-10-13	4.3	CVE-2008-3271 CONFIRM BID BUGTRAQ CONFIRM CONFIRM CONFIRM SECUNIA JVN

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- cups cups -- cups	Integer overflow in the WriteProlog function in texttops in CUPS before 1.3.9 allows remote attackers to execute arbitrary code via a crafted PostScript file that triggers a heap-based buffer overflow.	2008-10-14	6.8	CVE-2008-3640 SECTRACK BID REDHAT MANDRIVA FRSIRT CONFIRM CONFIRM SECUNIA SECUNIA
bea -- weblogic_workshop oracle -- weblogic_workshop	Unspecified vulnerability in the WebLogic Workshop component in BEA Product Suite WLW 8.1SP5 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2008-10-14	5.1	CVE-2008-4012 CONFIRM
ca -- arcserve_backup ca -- business_protection_suite ca -- server_protection_suite	Unspecified vulnerability in the tape engine service in asdbapi.dll in CA ARCserve Backup (formerly BrightStor ARCserve Backup) r11.1 through r12.0 allows remote attackers to cause a denial of service (crash) via a crafted request.	2008-10-14	5.0	CVE-2008-4398 CONFIRM
ca -- arcserve_backup ca -- business_protection_suite ca -- server_protection_suite	Unspecified vulnerability in the database engine service in asdbapi.dll in CA ARCserve Backup (formerly BrightStor ARCserve Backup) r11.1 through r12.0 allows remote attackers to cause a denial of service (crash) via a crafted request, related to "insufficient validation."	2008-10-14	5.0	CVE-2008-4399 CONFIRM
ca -- arcserve_backup ca -- business_protection_suite ca -- server_protection_suite	Unspecified vulnerability in asdbapi.dll in CA ARCserve Backup (formerly BrightStor ARCserve Backup) r11.1 through r12.0 allows remote attackers to cause a denial of service (crash of multiple services) via crafted authentication credentials, related to "insufficient validation."	2008-10-14	5.0	CVE-2008-4400 CONFIRM
chilkat_software -- mail	Insecure method vulnerability in Chilkat Mail 7.8 ActiveX control (ChilkatCert.dll) allows remote attackers to overwrite arbitrary files via a full pathname to the SaveLastError method.	2008-10-15	6.8	CVE-2008-4584 XF BID MILWORM
cisco -- unity	Unspecified vulnerability in an unspecified Microsoft API, as used by Cisco Unity and possibly other products, allows remote attackers to cause a denial of service by sending crafted packets to dynamic UDP	2008-10-13	5.0	CVE-2008-4544 MISC BID FRSIRT CISCO

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ports, related to a "processing error."			SECTRACK
cisco -- unity	Cisco Unity 4.x before 4.2(1)ES161, 5.x before 5.0(1)ES53, and 7.x before 7.0(2)ES8 uses weak permissions for the D:\CommServer\Reports directory, which allows remote authenticated users to obtain sensitive information by reading files in this directory.	2008-10-13	4.0	CVE-2008-4545 MISC BID FRSIRT CISCO SECTRACK SECUNIA
dovecot -- dovecot	The ACL plugin in Dovecot before 1.1.4 treats negative access rights as if they are positive access rights, which allows attackers to bypass intended access restrictions.	2008-10-15	6.4	CVE-2008-4577 FRSIRT MLIST
dovecot -- dovecot	The ACL plugin in Dovecot before 1.1.4 allows attackers to bypass intended access restrictions by using the "k" right to create unauthorized "parent/child/child" mailboxes.	2008-10-15	5.0	CVE-2008-4578 MLIST
ibm -- enovia_smarteam	The Editor in IBM ENOVIA SmarTeam 5 before release 18 SP5, and release 19 before SP01, allows remote authenticated users to bypass intended access restrictions and read Document objects via the Workflow Process (aka Flow Process) view.	2008-10-15	4.0	CVE-2008-4581 BID AIXAPAR CONFIRM SECUNIA
jdwards -- enterpriseone oracle -- jd_edwards_enterpriseone oracle -- peoplesoft_enterprise oracle -- peoplesoft_peopletools	Unspecified vulnerability in the PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.18 and 8.49.14 allows remote attackers to affect confidentiality and integrity via unknown vectors.	2008-10-14	6.4	CVE-2008-4000 CONFIRM
linux -- kernel	The do_splice_from function in fs/splice.c in the Linux kernel before 2.6.27 does not reject file descriptors that have the O_APPEND flag set, which allows local users to bypass append mode and make arbitrary changes to other locations in the file.	2008-10-15	4.6	CVE-2008-4554 MLIST MLIST CONFIRM CONFIRM
microsoft -- internet_explorer	Microsoft Internet Explorer 6 and 7 does not properly determine the domain or security zone of origin of web script, which allows remote attackers to bypass the intended cross-domain security policy and obtain sensitive information via a crafted	2008-10-14	4.3	CVE-2008-3474 MS

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HTML document, aka "Cross-Domain Information Disclosure Vulnerability."			
microsoft -- office	Cross-site scripting (XSS) vulnerability in Microsoft Office XP SP3 allows remote attackers to inject arbitrary web script or HTML via a document that contains a "Content-Disposition: attachment" header and is accessed through a cdo: URL, which renders the content instead of raising a File Download dialog box, aka "Vulnerability in Content-Disposition Header Vulnerability."	2008-10-14	4.3	CVE-2008-4020 MS
mozilla -- firefox	Mozilla Firefox 3.0.1 through 3.0.3 on Windows does not properly identify the context of Windows .url shortcut files, which allows user-assisted remote attackers to bypass the Same Origin Policy and obtain sensitive information via an HTML document that is directly accessible through a filesystem, as demonstrated by documents in (1) local folders, (2) Windows share folders, and (3) RAR archives, and as demonstrated by IFRAMEs referencing shortcuts that point to (a) about:cache?device=memory and (b) about:cache?device=disk, a variant of CVE-2008-2810.	2008-10-15	4.3	CVE-2008-4582 BUGTRAQ SECUNIA MISC
oracle -- database_10g	Unspecified vulnerability in the Oracle OLAP component in Oracle Database 10.1.0.5 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.	2008-10-14	6.5	CVE-2008-2624 CONFIRM
oracle -- database_10g oracle -- database_9i	Unspecified vulnerability in the Core RDBMS component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.2 allows remote attackers to affect confidentiality and integrity via unknown vectors.	2008-10-14	4.0	CVE-2008-2625 CONFIRM
oracle -- application_server	Unspecified vulnerability in the Oracle Portal component in Oracle Application Server 9.0.4.3 and 10.1.2.3 allows remote attackers to affect integrity via unknown vectors.	2008-10-14	5.0	CVE-2008-3975 CONFIRM
oracle -- database_10g oracle -- database_9i	Unspecified vulnerability in the Oracle Spatial component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.3	2008-10-14	5.5	CVE-2008-3976 CONFIRM

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows remote authenticated users to affect confidentiality and integrity via unknown vectors.			
oracle -- application_server	Unspecified vulnerability in the Oracle Portal component in Oracle Application Server 9.0.4.3 and 10.1.2.3 allows remote attackers to affect integrity via unknown vectors.	2008-10-14	5.0	CVE-2008-3977 CONFIRM
oracle -- database_10g	Unspecified vulnerability in the Upgrade component in Oracle Database 10.1.0.5 and 10.2.0.3 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2008-10-14	4.9	CVE-2008-3980 CONFIRM
oracle -- database_10g oracle -- database_11i oracle -- database_9i	Unspecified vulnerability in the Workspace Manager component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.3, and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity, related to SYS.LT and WMSYS.LT.	2008-10-14	5.5	CVE-2008-3982 CONFIRM
oracle -- database_10g oracle -- database_11i oracle -- database_9i	Unspecified vulnerability in the Workspace Manager component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.3, and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity, related to SYS.LT and WMSYS.LT.	2008-10-14	5.5	CVE-2008-3983 CONFIRM
oracle -- database_10g oracle -- database_11i oracle -- database_9i	Unspecified vulnerability in the Workspace Manager component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.3, and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity, related to SYS.LT and WMSYS.LT.	2008-10-14	5.5	CVE-2008-3984 CONFIRM
oracle -- e-business_suite	Unspecified vulnerability in the Oracle Applications Technology Stack component in Oracle E-Business Suite 12.0.4 allows remote attackers to affect confidentiality via unknown vectors.	2008-10-14	5.0	CVE-2008-3985 CONFIRM
oracle -- e-business_suite	Unspecified vulnerability in the iSupplier Portal component in Oracle E-Business Suite 11.5.10.2 and 12.0.4 allows remote attackers to affect confidentiality via unknown vectors.	2008-10-14	5.0	CVE-2008-3988 CONFIRM
oracle -- database_10g	Unspecified vulnerability in the Oracle Data Mining component in Oracle Database 10.2.0.3 allows remote authenticated users to affect	2008-10-14	6.5	CVE-2008-3989 CONFIRM

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	confidentiality, integrity, and availability, related to DMSYS.ODM_MODEL_UTIL.			
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 OLAPSYS.CWM2_OLAP_AW_AWUTIL.	2008-10-14	4.0	CVE-2008-3990 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 OLAPSYS.CWM2_OLAP_AW_AWUTIL.	2008-10-14	4.0	CVE-2008-3991 CONFIRM
oracle -- database_10g	Unspecified vulnerability in the Oracle Data Mining component in Oracle Database 10.2.0.4 allows remote authenticated users to affect confidentiality and integrity, related to DMSYS.DBMS_DM_EXP_INTERNAL.	2008-10-14	5.5	CVE-2008-3992 CONFIRM
oracle -- database_10g oracle -- database_11i oracle -- database_9i	Unspecified vulnerability in the Workspace Manager component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.3, and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity, related to WMSYS.LTADM.	2008-10-14	5.5	CVE-2008-3994 CONFIRM
oracle -- database_10g oracle -- database_11i	Unspecified vulnerability in the Change Data Capture component in Oracle Database 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_CDC_PUBLISH.	2008-10-14	5.5	CVE-2008-3995 CONFIRM
oracle -- database_10g oracle -- database_11i	Unspecified vulnerability in the Change Data Capture component in Oracle Database 10.1.0.5, 10.2.0.4, and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity, related to SYS.DBMS_CDC_IPUBLISH.	2008-10-14	5.5	CVE-2008-3996 CONFIRM
oracle -- e-business_suite	Unspecified vulnerability in the Oracle iStore component in Oracle E-Business Suite 12.0.4 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2008-10-14	4.9	CVE-2008-3998 CONFIRM

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- jd_edwards_enterpriseone_ep oracle -- peoplesoft_enterprise	Unspecified vulnerability in the PeopleSoft Enterprise Portal component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne EP 8.9 and EP 9.0 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2008-10-14	4.9	CVE-2008-4001 CONFIRM
oracle -- jd_edwards_enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.18 and 8.49.14 allows remote attackers to affect confidentiality via unknown vectors.	2008-10-14	4.3	CVE-2008-4003 CONFIRM
oracle -- database_11i	Unspecified vulnerability in the Oracle Application Express component in Oracle Database 11.1.0.6 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.	2008-10-14	4.3	CVE-2008-4005 CONFIRM
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 9.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2008-10-14	5.1	CVE-2008-4009 CONFIRM
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Workshop component in BEA Product Suite 10.3, 10.2, 10.0 MP1, 9.2 MP3, and 8.1 SP6 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2008-10-14	6.8	CVE-2008-4010 CONFIRM
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, 9.0, and 8.1 SP6 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2008-10-14	6.8	CVE-2008-4013 CONFIRM
phpwebgallery -- phpwebgallery	Multiple cross-site scripting (XSS) vulnerabilities in admin/include/isadmin.inc.php in PhpWebGallery 1.3.4 allow remote attackers to inject arbitrary web script or HTML via the (1) lang[access_forbiden] and (2) lang[ident_title] parameters.	2008-10-16	4.3	CVE-2008-4591 MILWORM
plone -- plone	Cross-site scripting (XSS) vulnerability in the LiveSearch module in Plone before	2008-10-15	4.3	CVE-2008-4571 BID

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	3.0.4 allows remote attackers to inject arbitrary web script or HTML via the Description field for search results, as demonstrated using the onerror Javascript even in an IMG tag.			CONFIRM
sentex -- jhead	Buffer overflow in the DoCommand function in jhead before 2.84 might allow context-dependent attackers to cause a denial of service (crash) via (1) a long -cmd argument and (2) possibly other unspecified vectors.	2008-10-15	5.0	CVE-2008-4575 CONFIRM CONFIRM MLIST
strongswan -- strongswan	strongSwan 4.2.6 and earlier allows remote attackers to cause a denial of service (daemon crash) via an IKE_SA_INIT message with a large number of NULL values in a Key Exchange payload, which triggers a NULL pointer dereference for the return value of the mpz_export function in the GNU Multiprecision Library (GMP).	2008-10-14	5.0	CVE-2008-4551 SECTRACK BID FRSIRT SECUNIA MISC CONFIRM
videolan -- vlc_media_player	Array index error in VLC media player 0.9.2 allows remote attackers to overwrite arbitrary memory and execute arbitrary code via an XSPF playlist file with a negative identifier tag, which passes a signed comparison.	2008-10-14	6.8	CVE-2008-4558 MISC

[Back to top](#)

Low Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- unity	Cross-site scripting (XSS) vulnerability in Cisco Unity 4.x before 4.2(1)ES162, 5.x before 5.0(1)ES56, and 7.x before 7.0(2)ES8 allows remote authenticated administrators to inject arbitrary web script or HTML by entering it in the database (aka data store).	2008-10-13	3.5	CVE-2008-4542 MISC BID FRSIRT CISCO SECTRACK SECUNIA
gentoo -- cman gentoo -- fence	The (1) fence_apc and (2) fence_apc_snmp programs, as used in (a) fence 2.02.00-r1 and possibly (b) cman, when running in verbose mode, allows local users to append to arbitrary files via a symlink attack on the apclog temporary file.	2008-10-15	1.9	CVE-2008-4579 MLIST MISC

[Back to top](#)

Low Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
imageshack -- imageshack_toolbar	The ImageShack Toolbar ActiveX control (ImageShackToolbar.dll) in ImageShack Toolbar 4.5.7, possibly including 4.5.7.69, allows remote attackers to force the upload of arbitrary image files to the ImageShack site via a file: URI argument to the BuildSlideShow method.	2008-10-14	2.6	CVE-2008-4549 XF BID BUGTRAQ MILWORM SECUNIA
jdwards -- enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the JDE EnterpriseOne Business Service Server component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.97.2.2 and 8.98.0.1 allows local users to affect confidentiality and integrity via unknown vectors.	2008-10-14	3.2	CVE-2008-4004 CONFIRM
microsoft -- windows_mobile	Windows Mobile 6 on the HTC Hermes device makes WLAN passwords available to an auto-completion mechanism for the password input field, which allows physically proximate attackers to bypass password authentication and obtain WLAN access.	2008-10-13	2.1	CVE-2008-4540 BUGTRAQ
oracle -- jdeveloper	Unspecified vulnerability in the Oracle JDeveloper component in Oracle Application Server 10.1.2.2 allows local users to affect confidentiality via unknown vectors.	2008-10-14	2.1	CVE-2008-2588 CONFIRM
oracle -- application_server oracle -- e-business_suite	Unspecified vulnerability in the Oracle Reports Developer component in Oracle Application Server 1.0.2.2, 9.0.4.3, and 10.1.2.2, and E-Business Suite 11.5.10.2, allows remote authenticated users to affect availability via unknown vectors.	2008-10-14	1.7	CVE-2008-2619 CONFIRM
oracle -- application_server	Unspecified vulnerability in the Oracle Discoverer Administrator component in Oracle Application Server 9.0.4.3 and 10.1.2.2 allows local users to affect confidentiality via unknown vectors.	2008-10-14	1.0	CVE-2008-3986 CONFIRM
oracle -- application_server	Unspecified vulnerability in the Oracle Discoverer Desktop component in Oracle Application Server 10.1.2.3 allows local users to affect confidentiality via unknown vectors.	2008-10-14	1.0	CVE-2008-3987 CONFIRM
oracle -- e-business_suite	Unspecified vulnerability in the Oracle Applications Framework component in Oracle E-Business Suite 11.5.10.2 and 12.0.4 allows remote authenticated users to affect integrity via unknown vectors.	2008-10-14	3.5	CVE-2008-3993 CONFIRM

[Back to top](#)

Low Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- jd_edwards_enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.18 and 8.49.14 allows remote authenticated users to affect confidentiality via unknown vectors.	2008-10-14	<u>3.5</u>	<u>CVE-2008-4002 CONFIRM</u>
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, and 9.0 allows remote authenticated users to affect integrity via unknown vectors.	2008-10-14	<u>2.1</u>	<u>CVE-2008-4011 CONFIRM</u>
<u>Back to top</u>				