Vulnerability Summary for the Week of March 17, 2008

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**
Apple -- Mac OS X Server Apple -- Mac OS X	Unspecified vulnerability in CUPS before 1.3.6 in Apple Mac OS X 10.5.2 has unknown impact and attack vectors related to "input validation."	unknown 2008-03-18	10.0	CVE-2008-0053 APPLE

Apple -- Mac OS X Server Apple -- Mac OS X	Apple Mac OS X 10.5.2 allows user-assisted attackers to cause a denial of servicr (crash) via a crafted Universal Disc Format (UDF) disk image, which triggers a NULL pointer dereference.	unknown 2008-03-18	7.1	CVE-2008-0999 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Directory traversal vulnerability in ContentServer.py in the Wiki Server in Apple Mac OS X 10.5.2 (aka Leopard) allows remote authenticated users to write arbitrary files via ".." sequences in file attachments.	unknown 2008-03-18	8.5	CVE-2008-1000 OTHER-REF
Advanced Data Solutions -- Virtual Support Office_XP	SQL injection vulnerability in MyIssuesView.asp in Advanced Data Solutions Virtual Support Office-XP (VSO-XP) allows remote attackers to execute arbitrary SQL commands via the Issue_ID parameter.	unknown 2008-03-17	7.5	CVE-2008-1354 BUGTRAQ BID SECUNIA
Apple -- Mac OS X Server Apple -- Mac OS X	Unspecified vulnerability in AFP Server in Apple Mac OS X 10.4.11 allows remote attackers to bypass cross-realm authentication via unknown manipulations of Kerberos principal realm names.	unknown 2008-03-18	7.1	CVE-2008-0045 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	CFNetwork in Apple Mac OS X 10.4.11 allows remote HTTPS proxy servers to spoof secure websites via data in a 502 Bad Gateway error	unknown 2008-03-18	7.8	CVE-2008-0050 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Foundation in Apple Mac OS X 10.4.11 creates world-writable directories while NSFileManager copies files recursively and only modifies the permissions afterward, which allows local users to modify copied files to cause a denial of service and possibly gain privileges.	unknown 2008-03-18	7.2	CVE-2008-0055 APPLE

Asterisk -- s800i Asterisk -- Asterisk Business Edition Asterisk -- Asterisk Appliance Developer Kit Asterisk -- AsteriskNOW Asterisk -- Open Source	Unspecified vulnerability in Asterisk Open Source 1.2.x before 1.2.27, 1.4.x before 1.4.18.1 and 1.4.19-rc3; Business Edition A.x.x, B.x.x before B.2.5.1, and C.x.x before C.1.6.2; AsteriskNOW 1.0.x before 1.0.2; Appliance Developer Kit before 1.4 revision 109393; and s800i 1.0.x before 1.1.0.2; allows remote attackers to access the SIP channel driver via a crafted From header.	unknown 2008-03-19	8.8	CVE-2008-1332 OTHER-REF
businessobjects -- Business Objects	Stack-based buffer overflow in the SAP Business Objects BusinessObjects RptViewerAX ActiveX control in RptViewerAX.dll in Business Objects 6.5 before CHF74 allows remote attackers to execute arbitrary code via unspecified vectors.	unknown 2008-03-19	9.3	CVE-2007-6254 OTHER-REF CERT-VN BID
cups -- CUPS	Heap-based buffer overflow in CUPS in Apple Mac OS X 10.5.2, when printer sharing is enabled, allows remote attackers to execute arbitrary code via crafted search expressions.	unknown 2008-03-18	10.0	CVE-2008-0047 APPLE
Easy-Clanpage -- Easy-Clanpage	SQL injection vulnerability in index.php in the gallery module in Easy-Clanpage 2.2 allows remote attackers to execute arbitrary SQL commands via the id parameter in a kate action.	unknown 2008-03-20	7.5	CVE-2008-1425 MILW0RM BID
Exero -- Exero CMS	Multiple directory traversal vulnerabilities in the Default theme in Exero CMS 1.0.1 allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the theme parameter to (1) index.php, (2) editpassword.php, and (3) avatar.php in usercp/; (4) custompage.php; (5) errors/404.php; (6) memberslist.php and (7) profile.php in members/; (8) index.php and (9) fullview.php in news/; and (10) nopermission.php.	unknown 2008-03-20	7.5	CVE-2008-1409 MILW0RM

exV2 -- BamaGalerie exV2 -- eXV2	SQL injection vulnerability in viewcat.php in the bamaGalerie (Bama Galerie) 3.03 and 3.041 module for eXV2 2.0.6 allows remote attackers to execute arbitrary SQL commands via the cid parameter.	unknown 2008-03-17	7.5	CVE-2008-1349 MILW0RM SECUNIA SECUNIA
Fully Modded phpBB -- Fully Modded phpBB	SQL injection vulnerability in kb.php in Fully Modded phpBB (phpbbfm) 80220 allows remote attackers to execute arbitrary SQL commands via the k parameter in an article action.	unknown 2008-03-17	7.5	CVE-2008-1350 BUGTRAQ MILW0RM BID SECUNIA
GNU -- gcc	gcc 4.3.x does not generate a cld instruction while compiling functions used for string manipulation such as memcpy and memmove on x86 and i386, which can prevent the direction flag (DF) from being reset in violation of ABI conventions and cause data to be copied in the wrong direction during signal handling in the Linux kernel, which might allow context-dependent attackers to trigger memory corruption. NOTE: this issue was originally reported for CPU consumption in SBCL.	unknown 2008-03-17	7.5	CVE-2008-1367 OTHER-REF OTHER-REF MLIST MLIST MLIST MLIST MLIST
HP -- StorageWorks Library and Tape Tools	HP StorageWorks Library and Tape Tools (LTT) before 4.5 SR1 on HP-UX B.11.11 and B.11.23 allows local users to gain privileges via unspecified vectors.	unknown 2008-03-19	7.2	CVE-2008-0707 HP SECTRACK SECUNIA
Iatek -- ASPapp	SQL injection vulnerability in links.asp in ASPapp allows remote attackers to execute arbitrary SQL commands via the CatId parameter.	unknown 2008-03-20	7.5	CVE-2008-1430 MILW0RM

IBM -- Informix Dynamic Server	Multiple buffer overflows in oninit.exe in IBM Informix Dynamic Server (IDS) 7.x through 11.x allow (1) remote attackers to execute arbitrary code via a long password and (2) remote authenticated users to execute arbitrary code via a long DBPATH value.	unknown 2008-03-17	8.5	CVE-2008-0727 BUGTRAQ BUGTRAQ OTHER-REF OTHER-REF AIXAPAR AIXAPAR AIXAPAR AIXAPAR BID FRSIRT SECUNIA XF XF
IBM -- Informix Dynamic Server	Unspecified vulnerability in IBM Informix Dynamic Server (IDS) 7.x through 11.x allows remote attackers to gain privileges via a malformed connection request packet.	unknown 2008-03-17	10.0	CVE-2008-0949 OTHER-REF OTHER-REF AIXAPAR AIXAPAR BID FRSIRT SECUNIA
Joobi -- Acajoom Joomla -- com_acajoom	SQL injection vulnerability in the Joobi Acajoom (com_acajoom) 1.1.5 and 1.2.5 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the mailingid parameter in a mailing view action to index.php.	unknown 2008-03-20	7.5	CVE-2008-1427 MILW0RM BID SECUNIA

KAPhotoservice -- KAPhotoservice	SQL injection vulnerability in album.asp in KAPhotoservice allows remote attackers to execute arbitrary SQL commands via the albumid parameter.	unknown 2008-03-20	7.5	CVE-2008-1426 MILW0RM BID SECUNIA
LaGarde -- StoreFront	SQL injection vulnerability in SearchResults.aspx in LaGarde StoreFront 6 before SP8 allows remote attackers to execute arbitrary SQL commands via the CategoryId parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-17	7.5	CVE-2008-1341 BID SECUNIA
MG-Soft -- Net Inspector	MG-SOFT Net Inspector 6.5.0.828 and earlier for Windows allows remote attackers to cause a (1) denial of service (exception and crash) via a UDP packet to the SNMP Trap Service (MgWTrap3.exe) or (2) denial of service (device freeze or memory consumption) via a malformed TCP packet to the Net Inspector Server (niengine).	unknown 2008-03-20	7.1	CVE-2008-1402 OTHER-REF SECUNIA
MIT -- Kerberos 5	KDC in MIT Kerberos 5 (krb5kdc) does not set a global variable for some krb4 message types, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted messages that trigger a NULL pointer dereference or double-free.	unknown 2008-03-19	9.3	CVE-2008-0062 BUGTRAQ OTHER-REF OTHER-REF APPLE CERT-VN
MIT -- Kerberos 5	Buffer overflow in the RPC library used by libgssrpc and kadmind in MIT Kerberos 5 (krb5) 1.4 through 1.6.3 allows remote attackers to execute arbitrary code by triggering a large number of open file descriptors.	unknown 2008-03-18	10.0	CVE-2008-0947 BUGTRAQ BUGTRAQ OTHER-REF CERT-VN

MIT -- Kerberos 5	Buffer overflow in the RPC library (lib/rpc/rpc_dtablesize.c) used by libgssrpc and kadmind in MIT Kerberos 5 (krb5) 1.2.2, and probably other versions before 1.3, when running on systems whose unistd.h library does not define the FD_SETSIZE macro, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by triggering a large number of open file descriptors.	unknown 2008-03-18	9.3	CVE-2008-0948 BUGTRAQ BUGTRAQ OTHER-REF CERT-VN
MyioSoft -- EasyCalendar	Multiple SQL injection vulnerabilities in MyioSoft EasyCalendar 4.0tr and earlier allow remote attackers to execute arbitrary SQL commands via the (1) year parameter in a dayview action to plugins/calendar/calendar_backend.php and the (2) page parameter to ajaxp_backend.php.	unknown 2008-03-17	7.5	CVE-2008-1344 MILW0RM BID SECUNIA
MyioSoft -- EasyCalendar	SQL injection vulnerability in staticpages/easygallery/index.php in MyioSoft EasyGallery 5.0tr and earlier allows remote attackers to execute arbitrary SQL commands via the catid parameter in a category action.	unknown 2008-03-17	7.5	CVE-2008-1346 MILW0RM BID SECUNIA
phpBP -- phpBP	SQL injection vulnerability in includes/functions/banners-external.php in phpBP 2 RC3 (2.204) FIX 4 allows remote attackers to execute arbitrary SQL commands via the id parameter in a banner_out action.	unknown 2008-03-20	7.5	CVE-2008-1408 MILW0RM OTHER-REF OTHER-REF SECUNIA

Plone -- Plone CMS	Plone CMS 3.0.5, and probably other 3.x versions, places a base64 encoded form of the username and password in the __ac cookie for the admin account, which makes it easier for remote attackers to obtain administrative privileges by sniffing the network.	unknown 2008-03-19	10.0	CVE-2008-1393 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF
Plone -- Plone CMS	Plone CMS before 3 places a base64 encoded form of the username and password in the __ac cookie for all user accounts, which makes it easier for remote attackers to obtain access by sniffing the network.	unknown 2008-03-19	7.5	CVE-2008-1394 BUGTRAQ OTHER-REF OTHER-REF
Plone -- Plone CMS	Plone CMS does not record users' authentication states, and implements the logout feature solely on the client side, which makes it easier for context-dependent attackers to reuse a logged-out session.	unknown 2008-03-19	7.5	CVE-2008-1395 BUGTRAQ OTHER-REF
rPath -- rPath Linux	The NEEDBITS macro in the inflate_dynamic function in inflate.c for unzip can be invoked using invalid buffers, which allows remote attackers to cause a denial of service (crash) and possible execute arbitrary code via unknown vectors that trigger a free of uninitialized or previously-freed data.	unknown 2008-03-17	9.4	CVE-2008-0888 OTHER-REF
SILC -- SILC-Server	Secure Internet Live Conferencing (SILC) Server before 1.1.1 allows remote attackers to cause a denial of service (daemon crash) via a NEW_CLIENT packet without a nickname.	unknown 2008-03-20	7.8	CVE-2008-1429 OTHER-REF FRSIRT

Sun -- Solaris	A certain incorrect Sun Solaris 10 image on SPARC Enterprise T5120 and T5220 servers has /etc/default/login and /etc/ssh/sshd_config files that configure root logins in a manner unintended by the vendor, which allows remote attackers to gain privileges via unspecified vectors.	unknown 2008-03-18	10.0	CVE-2008-1369 FRSIRT
VMWare -- VMWare Workstation VMWare -- ACE VMWare -- VMware Server VMWare -- Player	Virtual Machine Communication Interface (VMCI) in VMware Workstation 6.0.x before 6.0.3, VMware Player 2.0.x before 2.0.3, and VMware ACE 2.0.x before 2.0.1 allows attackers to cause a denial of service (host OS crash) via crafted VMCI calls that trigger "memory exhaustion and memory corruption."	unknown 2008-03-19	7.1	CVE-2008-1340 BUGTRAQ MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID SECTRACK
VMWare -- VMWare Workstation VMWare -- ACE VMWare -- VMware Server VMWare -- Player	VMware Workstation 6.0.x before 6.0.3 and 5.5.x before 5.5.6, VMware Player 2.0.x before 2.0.3 and 1.0.x before 1.0.6, VMware ACE 2.0.x before 2.0.1 and 1.0.x before 1.0.5, and VMware Server 1.0.x before 1.0.5 on Windows allow local users to gain privileges via an unspecified manipulation that causes the authd process to connect to an arbitrary named pipe, a different vulnerability than CVE-2008-1362.	unknown 2008-03-19	7.2	CVE-2008-1361 BUGTRAQ MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-

				REF BID SECTRACK
VMWare -- VMWare Workstation VMWare -- ACE VMWare -- VMware Server VMWare -- Player	VMware Workstation 6.0.x before 6.0.3 and 5.5.x before 5.5.6, VMware Player 2.0.x before 2.0.3 and 1.0.x before 1.0.6, VMware ACE 2.0.x before 2.0.1 and 1.0.x before 1.0.5, and VMware Server 1.0.x before 1.0.5 on Windows allow local users to gain privileges or cause a denial of service by impersonating the authd process through an unspecified use of an "insecurely created named pipe," a different vulnerability than CVE-2008-1361.	unknown 2008-03-19	7.2	CVE-2008-1362 BUGTRAQ MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID SECTRACK
VMWare -- VMWare Workstation VMWare -- ACE VMWare -- VMware Server VMWare -- Player	VMware Workstation 6.0.x before 6.0.3 and 5.5.x before 5.5.6, VMware Player 2.0.x before 2.0.3 and 1.0.x before 1.0.6, VMware ACE 2.0.x before 2.0.1 and 1.0.x before 1.0.5, and VMware Server 1.0.x before 1.0.5 on Windows allow local users to gain privileges via an unspecified manipulation of a config.ini file located in an Application Data folder, which can be used for "hijacking the VMX process."	unknown 2008-03-19	7.2	CVE-2008-1363 BUGTRAQ MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-

				REF OTHER-REF BID SECTRACK
VMWare -- VMWare Workstation VMWare -- ACE VMWare -- VMware Server VMWare -- Player	Unspecified vulnerability in the DHCP service in VMware Workstation 5.5.x before 5.5.6, VMware Player 1.0.x before 1.0.6, VMware ACE 1.0.x before 1.0.5, VMware Server 1.0.x before 1.0.5, and VMware Fusion 1.1.x before 1.1.1 allows attackers to cause a denial of service.	unknown 2008-03-19	7.8	CVE-2008-1364 BUGTRAQ MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID SECTRACK
VMWare -- VMWare Workstation VMWare -- ACE VMWare -- Player	The default configuration of VMware Workstation 6.0.2, VMware Player 2.0.x before 2.0.3, and VMware ACE 2.0.x before 2.0.1 makes the console of the guest OS accessible through anonymous VIX API calls, which has unknown impact and attack vectors.	unknown 2008-03-19	10.0	CVE-2008-1392 BUGTRAQ MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID

XOOPS -- Tutoriais Module	SQL injection vulnerability in the Tutorials 2.1b module for XOOPS allows remote attackers to execute arbitrary SQL commands via the tid parameter to printpage.php, which is accessible directly or through a printpage action to index.php.	unknown 2008-03-17	7.5	CVE-2008-1351 MILW0RM SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Acronis -- Snap_Deploy	Directory traversal vulnerability in the PXE Server (pxesrv.exe) in Acronis Snap Deploy 2.0.0.1076 and earlier allows remote attackers to read arbitrary files via directory traversal sequences to the TFTP service.	unknown 2008-03-20	4.3	CVE-2008-1410 BUGTRAQ MILW0RM OTHER-REF BID FRSIRT SECUNIA XF
Acronis -- Snap_Deploy	The PXE Server (pxesrv.exe) in Acronis Snap Deploy 2.0.0.1076 and earlier allows remote attackers to cause a denial of service (crash) via an incomplete TFTP request, which triggers a NULL pointer dereference.	unknown 2008-03-20	5.0	CVE-2008-1411 BUGTRAQ MILW0RM OTHER-REF BID FRSIRT SECUNIA XF

Alt-N -- MDaemon	Sack-based buffer overflow in the IMAP server in Alt-N Technologies MDaemon 9.6.4 allows remote authenticated users to execute arbitrary code via a FETCH command with a long BODY.	unknown 2008-03-17	6.5	CVE-2008-1358 MILW0RM OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Apple -- Mac OS X Server Apple -- Mac OS X	Multiple buffer overflows in AFP Client in Apple Mac OS X 10.4.11 and 10.5.2 allow remote attackers to cause a denial of service (application termination) and execute arbitrary code via a crafted afp:// URL.	unknown 2008-03-18	5.8	CVE-2008-0044 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	The Application Firewall in Apple Mac OS X 10.5.2 has an incorrect German translation for the "Set access for specific services and applications" radio button that might cause the user to believe that the button is used to restrict access only to specific services and applications, which might allow attackers to bypass intended access restrictions.	unknown 2008-03-18	5.0	CVE-2008-0046 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Stack-based buffer overflow in AppKit in Apple Mac OS X 10.4.11 allows context-dependent attackers to execute arbitrary code via the a long file name to the NSDocument API.	unknown 2008-03-18	6.8	CVE-2008-0048 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Integer overflow in CoreFoundation in Apple Mac OS X 10.4.11 might allow local users to execute arbitrary code via crafted time zone data.	unknown 2008-03-18	6.9	CVE-2008-0051 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	CoreServices in Apple Mac OS X 10.4.11 treats .ief as a safe file type, which allows remote attackers to force Safari users into opening an .ief file in AppleWorks, even when the "Open 'Safe' files" preference is set.	unknown 2008-03-18	6.8	CVE-2008-0052 APPLE

Apple -- Mac OS X Server Apple -- Mac OS X	Foundation in Apple Mac OS X 10.4.11 might allow context-dependent attackers to execute arbitrary code via a malformed selector name to the NSSelectorFromString API, which causes an "unexpected selector" to be used.	unknown 2008-03-18	6.4	CVE-2008-0054 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Stack-based buffer overflow in Foundation in Apple Mac OS X 10.4.11 allows context-dependent attackers to execute arbitrary code via a "long pathname with an unexpected structure" that triggers the overflow in NSFileManager.	unknown 2008-03-18	6.8	CVE-2008-0056 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Multiple integer overflows in a "legacy serialization format" parser in AppKit in Apple Mac OS X 10.4.11 allows remote attackers to execute arbitrary code via a crafted serialized property list	unknown 2008-03-18	6.8	CVE-2008-0057 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Race condition in the NSURLConnection cache management functionality in Foundation for Apple Mac OS X 10.4.11 allows remote attackers to execute arbitrary code via unspecified manipulations that cause messages to be sent to a deallocated object.	unknown 2008-03-18	5.8	CVE-2008-0058 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Race condition in NSXML in Foundation for Apple Mac OS X 10.4.11 allows context-dependent attackers to execute arbitrary code via a crafted XML file, related to "error handling logic."	unknown 2008-03-18	5.8	CVE-2008-0059 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Help Viewer in Apple Mac OS X 10.4.11 and 10.5.2 allows remote attackers to execute arbitrary Applescript via a help: topic_list URL that injects HTML or JavaScript into a topic list page, as demonstrated using a help:runscript link.	unknown 2008-03-18	6.8	CVE-2008-0060 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Stack-based buffer overflow in Image Raw in Apple Mac OS X 10.5.2 allows remote attackers to execute arbitrary code via a crafted Adobe Digital Negative (DNG) image.	unknown 2008-03-18	6.8	CVE-2008-0987 APPLE

Apple -- Mac OS X Server Apple -- Mac OS X	Off-by-one error in the Libsystem strnstr API in libc on Apple Mac OS X 10.4.11 allows context-dependent attackers to cause a denial of service (crash) via crafted arguments that trigger a buffer over-read.	unknown 2008-03-18	4.3	CVE-2008-0988 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Format string vulnerability in mDNSResponderHelper in Apple Mac OS X 10.5.2 allows local users to execute arbitrary code via format string specifiers in the local hostname.	unknown 2008-03-18	6.9	CVE-2008-0989 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	notifyd in Apple Mac OS X 10.4.11 does not verify that Mach port death notifications have originated from the kernel, which allows local users to cause a denial of service via spoofed death notifications that prevent other applications from receiving notifications.	unknown 2008-03-18	4.4	CVE-2008-0990 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Array index error in pax in Apple Mac OS X 10.5.2 allows context-dependent attackers to execute arbitrary code via an archive with a crafted length value.	unknown 2008-03-18	5.8	CVE-2008-0992 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Stack-based buffer overflow in AppKit in Apple Mac OS X 10.4.11 allows user-assisted remote attackers to cause a denial of service (application termination) and execute arbitrary code via a crafted PostScript Printer Description (PPD) file that is not properly handled when querying a network printer.	unknown 2008-03-18	6.8	CVE-2008-0997 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	Unspecified vulnerability in NetCfgTool in the System Configuration component in Apple Mac OS X 10.4.11 and 10.5.2 allows local users to bypass authorization and execute arbitrary code via crafted distributed objects.	unknown 2008-03-18	6.9	CVE-2008-0998 APPLE

Apple -- Safari	Cross-site scripting (XSS) vulnerability in Apple Safari before 3.1, when running on Windows XP or Vista, allows remote attackers to inject arbitrary web script or HTML via a crafted URL that is not properly handled in the error page.	unknown 2008-03-18	4.3	CVE-2008-1001 APPLE
Apple -- Safari	Cross-site scripting (XSS) vulnerability in Apple Safari before 3.1 allows remote attackers to inject arbitrary web script or HTML via a crafted javascript: URL.	unknown 2008-03-18	4.3	CVE-2008-1002 APPLE
Apple -- Safari	Cross-site scripting (XSS) vulnerability in WebCore, as used in Apple Safari before 3.1, allows remote attackers to inject arbitrary web script or HTML via unknown vectors related to sites that set the document.domain property or have the same document.domain.	unknown 2008-03-18	4.3	CVE-2008-1003 APPLE
Apple -- Safari	Cross-site scripting (XSS) vulnerability in WebCore, as used in Apple Safari before 3.1, allows remote attackers to inject arbitrary web script or HTML via unknown vectors related to the Web Inspector.	unknown 2008-03-18	4.3	CVE-2008-1004 APPLE
Apple -- Safari	Cross-site scripting (XSS) vulnerability in WebCore, as used in Apple Safari before 3.1, allows remote attackers to inject arbitrary web script or HTML by using the window.open function to change the security context of a web page.	unknown 2008-03-18	4.3	CVE-2008-1006 APPLE
Apple -- Safari	WebCore, as used in Apple Safari before 3.1, does not enforce the frame navigation policy for Java applets, 2which allows remote attackers to conduct cross-site scripting (XSS) attacks.	unknown 2008-03-18	4.3	CVE-2008-1007 APPLE
Apple -- Safari	Cross-site scripting (XSS) vulnerability in WebCore, as used in Apple Safari before 3.1, allows remote attackers to inject arbitrary web script or HTML via the document.domain property.	unknown 2008-03-18	4.3	CVE-2008-1008 APPLE

Apple -- Safari	Cross-site scripting (XSS) vulnerability in WebCore, as used in Apple Safari before 3.1, allows remote attackers to inject arbitrary JavaScript by modifying the history object.	unknown 2008-03-18	4.3	CVE-2008-1009 APPLE
Apple -- Safari	Buffer overflow in WebKit, as used in Apple Safari before 3.1, allows remote attackers to execute arbitrary code via crafted regular expressions in JavaScript.	unknown 2008-03-18	6.8	CVE-2008-1010 APPLE
Apple -- Safari	Cross-site scripting (XSS) vulnerability in WebKit, as used in Apple Safari before 3.1, allows remote attackers to inject arbitrary web script or HTML via a frame that calls a method instance in another frame.	unknown 2008-03-18	4.3	CVE-2008-1011 APPLE
Apple -- Apple AirPort Extreme Base Station	Unspecified vulnerability in Apple AirPort Extreme Base Station Firmware 7.3.1 allows remote attackers to cause a denial of service (file sharing hang) via a crafted AFP request, related to "input validation."	unknown 2008-03-20	4.3	CVE-2008-1012 OTHER-REF
Asterisk -- Open Source	Format string vulnerability in Asterisk Open Source 1.6.x before 1.6.0-beta6 might allow remote attackers to execute arbitrary code via logging messages that are not properly handled by (1) the ast_verbose logging API call, or (2) the astman_append function.	unknown 2008-03-19	5.8	CVE-2008-1333 OTHER-REF
auraCMS -- AuraCMS	SQL injection vulnerability in online.php in AuraCMS 2.0 through 2.2.1 allows remote attackers to execute arbitrary SQL commands via the X-Forwarded-For field (HTTP_X_FORWARDED_FOR environment variable) in an HTTP header.	unknown 2008-03-20	6.8	CVE-2008-1398 MILW0RM BID XF
Axyl -- Axyl	The prerm script in axyl 2.1.7 allows local users to overwrite arbitrary files via a symlink attack on the axyl.conf temporary file.	unknown 2008-03-20	4.6	CVE-2008-1417 OTHER-REF

BootManage -- TFTPD BootManage -- Administrator	Stack-based buffer overflow in the TFTP server in BootManage TFTPD 1.99 and earlier in BootManage Administrator 7.1 and earlier allows remote attackers to execute arbitrary code via a request with a long filename.	unknown 2008-03-20	6.8	CVE-2008-1403 OTHER-REF SECUNIA
bzip -- bzip2	bzlib.c in bzip2 before 1.0.5 allows user-assisted remote attackers to cause a denial of service (crash) via a crafted file that triggers a buffer over-read, as demonstrated by the PROTOS GENOME test suite.	unknown 2008-03-18	4.3	CVE-2008-1372 OTHER-REF OTHER-REF OTHER-REF CERT-VN BID FRSIRT
Checkpoint -- VPN-1 Power_UTM with NGX Checkpoint -- VPN-1 Power_UTM Checkpoint -- VPN-1 Firewall-1 Checkpoint -- Check Point VPN-1 Pro	Check Point VPN-1 Power/UTM, with NGX R60 through R65 and NG AI R55 software, allows remote authenticated users to cause a denial of service (site-to-site VPN tunnel outage), and possibly intercept network traffic, by configuring the local RFC1918 IP address to be the same as one of this tunnel's endpoint RFC1918 IP addresses, and then using SecuRemote to connect to a network interface at the other endpoint.	unknown 2008-03-19	6.5	CVE-2008-1397 OTHER-REF OTHER-REF CERT-VN BID SECUNIA
Clansphere -- Clansphere	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Clansphere 2008 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-20	4.3	CVE-2008-1399 BID XF

Drupal -- Ubercart Module	Multiple cross-site scripting (XSS) vulnerabilities in the Ubercart 5.x before 5.x-1.0-beta7 module for Drupal allow remote attackers to inject arbitrary web script or HTML via a text attribute value for a product.	unknown 2008-03-20	4.3	CVE-2008-1428 OTHER-REF FRSIRT XF
ewebsite -- eWeather	Cross-site scripting (XSS) vulnerability in index.php in the eWebsite eWeather (Weather) module for PHP-Nuke allows remote attackers to inject arbitrary web script or HTML via the chart parameter to modules.php.	unknown 2008-03-17	4.3	CVE-2008-1348 BUGTRAQ BID
exV2 -- eXV2	SQL injection vulnerability in index.php in the Viso (Industry Book) 2.04 and 2.03 module for eXV2 allows remote attackers to execute arbitrary SQL commands via the kid parameter.	unknown 2008-03-20	6.8	CVE-2008-1404 MILW0RM BID SECUNIA XF
exV2 -- eXV2	SQL injection vulnerability in annonces-p-f.php in the MyAnnonces 1.8 module for eXV2 allows remote attackers to execute arbitrary SQL commands via the lid parameter in an ImprAnn action.	unknown 2008-03-20	6.8	CVE-2008-1406 MILW0RM BID SECUNIA XF
exV2 -- eXV2	SQL injection vulnerability in index.php in the WebChat 1.60 module for eXV2 allows remote attackers to execute arbitrary SQL commands via the roomid parameter.	unknown 2008-03-20	6.8	CVE-2008-1407 MILW0RM BID SECUNIA XF

F-Secure -- F-Secure Mobile Antivirus for S60 F-Secure -- F-Secure Internet Security F-Secure -- F-Secure Mobile Antivirus for Windows Mobile F-Secure -- F-Secure Anti-Virus Client Security F-Secure -- F-Secure Protection Service for Business F-Secure -- F-Secure Anti-Virus F-Secure -- F-Secure Client Security F-Secure -- F-Secure Mobile Security for Series 80 F-Secure -- F-Secure Anti-Virus for Linux F-Secure -- F-Secure Anti-Virus for Workstations F-Secure -- F-Secure Anti-Virus Linux Client Security F-Secure -- F-Secure Protection Service for Consumers	Unspecified vulnerability in multiple F-Secure anti-virus products, including Internet Security 2006 through 2008, Anti-Virus 2006 through 2008, and others, allows remote attackers to execute arbitrary code or cause a denial of service (hang or crash) via a malformed archive that triggers an unhandled exception, as demonstrated by the PROTOS GENOME test suite for Archive Formats.	unknown 2008-03-20	6.8	CVE-2008-1412 OTHER-REF OTHER-REF FRSIRT SECUNIA

fuzzylime -- fuzzylime (cms)	PHP remote file inclusion vulnerability in code/display.php in fuzzylime cms 3.01 allows remote attackers to execute arbitrary PHP code via a URL in the admindir parameter.	unknown 2008-03-20	6.8	CVE-2008-1405 MILW0RM SECUNIA
Hangzhou Network Technology Development -- EdiorCMS	Directory traversal vulnerability in search.php in EdiorCMS (ecms) 3.0 allows remote attackers to read arbitrary files via a .. (dot dot) in the SearchTemplate parameter during a Title search.	unknown 2008-03-17	5.0	CVE-2008-1352 BUGTRAQ BID
IBM -- Rational ClearQuest	Multiple cross-site scripting (XSS) vulnerabilities in the web interface for IBM Rational ClearQuest before 2003.06.16 Patch 2008A, 7.0.0.2_iFix01, and 7.0.1.1_iFix01 allow remote attackers to inject arbitrary web script or HTML via the (1) contextid, (2) username, and userNameVal parameters to the login component.	unknown 2008-03-19	4.3	CVE-2007-4592 BUGTRAQ BID
Invision Power Services -- Invision Power Board	Cross-site scripting (XSS) vulnerability in Invision Power Board (IPB or IP.Board) 2.3.4 before 2008-03-13 allows remote attackers to inject arbitrary web script or HTML via nested BBCodes, a different vector than CVE-2008-0913.	unknown 2008-03-17	4.3	CVE-2008-1359 OTHER-REF SECUNIA
jeeblestechnology -- Jeebles Directory	Cross-site scripting (XSS) vulnerability in index.php in Jeebles Technology Jeebles Directory 2.9.60 allows remote attackers to inject arbitrary web script or HTML via the path parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-17	4.3	CVE-2008-1355 OTHER-REF BID XF

ManageEngine -- SupportCenter Plus	Cross-site scripting (XSS) vulnerability in SolutionSearch.do in ManageEngine SupportCenter Plus 7.0.0 allows remote attackers to inject arbitrary web script or HTML via the searchText parameter, a related issue to CVE-2008-1299. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-20	4.3	CVE-2008-1432 SECUNIA
McAfee -- CMA McAfee -- Agent McAfee -- McAfee Framework McAfee -- ePolicy Orchestrator	Format string vulnerability in the logDetail function of applib.dll in McAfee Common Management Agent (CMA) 3.6.0.574 (Patch 3) and earlier, as used in ePolicy Orchestrator 4.0.0 build 1015, allows remote attackers to cause a denial of service (crash) or execute arbitrary code via format string specifiers in a sender field in an AgentWakeup request to UDP port 8082. NOTE: this issue only exists when the debug level is 8.	unknown 2008-03-17	5.4	CVE-2008-1357 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
MG-Soft -- Net Inspector	Directory traversal vulnerability in the Net Inspector HTTP Server (mghttpd) in MG-SOFT Net Inspector 6.5.0.828 and earlier for Windows allows remote attackers to read arbitrary files via a "..\" (dot dot backslash) or "../" (dot dot slash) in the GET command.	unknown 2008-03-20	5.0	CVE-2008-1400 OTHER-REF SECUNIA
MG-Soft -- Net Inspector	Format string vulnerability in the Net Inspector HTTP server (mghttpd) in MG-SOFT Net Inspector 6.5.0.828 and earlier for Windows allows remote attackers to execute arbitrary code via format string specifiers in an HTTP GET request, which is recorded in a log file.	unknown 2008-03-20	4.3	CVE-2008-1401 OTHER-REF SECUNIA

Microsoft -- Internet Explorer	CRLF injection vulnerability in Microsoft Internet Explorer 5 and 6 allows remote attackers to execute arbitrary FTP commands via an ftp:// URL that contains a URL-encoded CRLF (%0D%0A) before the FTP command, which causes the commands to be inserted into an authenticated FTP connection established earlier in the same browser session, as demonstrated using a DELE command, a variant or possibly a regression of CVE-2004-1166. NOTE: a trailing "//" can force Internet Explorer to try to reuse an existing authenticated connection.	unknown 2008-03-17	4.3	CVE-2008-1368 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
MIT -- Kerberos 5	The Kerberos 4 support in KDC in MIT Kerberos 5 (krb5kdc) does not properly clear the unused portion of a buffer when generating an error message, which might allow remote attackers to obtain sensitive information, aka ""Uninitialized stack values."	unknown 2008-03-19	4.3	CVE-2008-0063 BUGTRAQ OTHER-REF OTHER-REF APPLE
MyioSoft -- EasyCalendar	Cross-site scripting (XSS) vulnerability in plugins/calendar/calendar_backend.php in MyioSoft EasyCalendar 4.0tr and earlier allows remote attackers to inject arbitrary web script or HTML via the day parameter in a dayview action.	unknown 2008-03-17	4.3	CVE-2008-1345 MILW0RM BID SECUNIA
MyioSoft -- EasyCalendar	Multiple cross-site scripting (XSS) vulnerabilities in staticpages/easygallery/index.php in MyioSoft EasyGallery 5.0tr and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the PATH_INFO or (2) the q parameter in an about action to the help system.	unknown 2008-03-17	4.3	CVE-2008-1347 MILW0RM BID SECUNIA

Nagios -- Nagios	Cross-site scripting (XSS) vulnerability in Nagios before 2.11 allows remote attackers to inject arbitrary web script or HTML via unknown vectors to unspecified CGI scripts, a different issue than CVE-2007-5624.	unknown 2008-03-17	4.3	CVE-2008-1360 OTHER-REF BID SECUNIA
PHPauction -- PHPauction GPL	Multiple PHP remote file inclusion vulnerabilities in PHPauction GPL 2.51 allow remote attackers to execute arbitrary PHP code via a URL in the include_path parameter to (1) converter.inc.php, (2) messages.inc.php, and (3) settings.inc.php in includes/.	unknown 2008-03-20	6.8	CVE-2008-1416 MILW0RM
Plone -- Plone CMS	Multiple cross-site request forgery (CSRF) vulnerabilities in Plone CMS 3.0.5 and 3.0.6 allow remote attackers to (1) add arbitrary accounts via the join_form page and (2) change the privileges of arbitrary groups via the prefs_groups_overview page.	unknown 2008-03-19	4.3	CVE-2008-0164 BUGTRAQ OTHER-REF OTHER-REF SECUNIA
Plone -- Plone CMS	Plone CMS 3.x uses invariant data (a client username and a server secret) when calculating an HMAC-SHA1 value for an authentication cookie, which makes it easier for remote attackers to gain permanent access to an account by sniffing the network.	unknown 2008-03-19	4.3	CVE-2008-1396 BUGTRAQ OTHER-REF
Polymita Technologies -- BPM_Suite Polymita Technologies -- CollagePortal	Multiple cross-site scripting (XSS) vulnerabilities in the search feature in Polymita BPM-Suite and CollagePortal allow remote attackers to inject arbitrary web script or HTML via the (1) _q and (2) lucene_index_field_value parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-17	4.3	CVE-2008-1342 SECUNIA

Riceball -- Multiple Time Sheets	Cross-site scripting (XSS) vulnerability in Multiple Time Sheets (MTS) 5.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the tab parameter to (1) index.php, as demonstrated using mixed case and encoded whitespace characters in the tag; or (2) clientinfo.php, (3) invoices.php, (4) smartlinks.php, and (5) todo.php, as demonstrated using a META tag.	unknown 2008-03-20	4.3	CVE-2008-1414 BUGTRAQ MILW0RM BID SECUNIA
Riceball -- Multiple Time Sheets	Directory traversal vulnerability in index. php in Multiple Time Sheets (MTS) 5.0 and earlier allows remote attackers to read arbitrary files via "../..//" (modified dot dot) sequences in the tab parameter.	unknown 2008-03-20	5.0	CVE-2008-1415 BUGTRAQ MILW0RM BID
SCO -- UnixWare	Directory traversal vulnerability in pkgadd and pkgrm in SCO UnixWare 7.1.4 allows local users to gain privileges via unknown vectors.	unknown 2008-03-17	4.9	CVE-2008-1343 SCO SECUNIA
sNews -- sNews CMS Rus	Cross-site scripting (XSS) vulnerability in search.php in SNewsCMS Rus 2.1 through 2.4 allows remote attackers to inject arbitrary web script or HTML via the query parameter.	unknown 2008-03-20	4.3	CVE-2008-1413 BUGTRAQ BID
Sun -- Solaris	Unspecified vulnerability in xscreensaver in Sun Solaris 10 Java Desktop System (JDS), when using the GNOME On-Screen Keyboard (GOK), allows local users to bypass authentication via unknown vectors that cause the screen saver to crash.	unknown 2008-03-17	6.3	CVE-2008-1356 SUNALERT BID FRSIRT SECUNIA XF

Trend Micro -- OfficeScan Corporate Edition	Stack-based buffer overflow in Trend Micro OfficeScan Corporate Edition 8.0 Patch 2 build 1189 and earlier, and 7.3 Patch 3 build 1314 and earlier, allows remote attackers to execute arbitrary code or cause a denial of service (crash) via a long encrypted password, which triggers the overflow in (1) cgiChkMasterPwd.exe, (2) policyserver.exe as reachable through cgiABLogon.exe, and other vectors.	unknown 2008-03-17	6.4	CVE-2008-1365 OTHER-REF SECUNIA
Trend Micro -- OfficeScan Corporate Edition	Trend Micro OfficeScan Corporate Edition 8.0 Patch 2 build 1189 and earlier, and 7.3 Patch 3 build 1314 and earlier, allows remote attackers to cause a denial of service (process consumption) via (1) an HTTP request without a Content-Length header or (2) invalid characters in unspecified CGI arguments, which triggers a NULL pointer dereference.	unknown 2008-03-17	5.0	CVE-2008-1366 OTHER-REF SECUNIA
Wildmary -- Yap Blog	PHP remote file inclusion vulnerability in index.php in wildmary Yap Blog 1.1 allows remote attackers to execute arbitrary PHP code via a URL in the page parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-18	6.8	CVE-2008-1370 BID XF
ZABBIX -- ZABBIX	zabbix_agentd in ZABBIX 1.4.4 allows remote attackers to cause a denial of service (CPU and connection consumption) via multiple vfs.file.cksum commands with a special device node such as /dev/urandom or /dev/zero.	unknown 2008-03-17	4.3	CVE-2008-1353 BUGTRAQ BID FRSIRT SECUNIA XF

Back to top

Low Vulnerabilities

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

	Preview in Apple Mac OS X 10.5.2 uses 40-bit RC4 when saving a PDF file with encryption, which makes it easier for attackers to decrypt the file via brute force methods.	unknown 2008-03-18	2.6	CVE-2008-0994 APPLE
	The Printing component in Apple Mac OS X 10.5.2 uses 40-bit RC4 when printing to an encrypted PDF file, which makes it easier for attackers to decrypt the file via brute force methods.	unknown 2008-03-18	2.6	CVE-2008-0995 APPLE
	The Printing component in Apple Mac OS X 10.5.2 might save authentication credentials to disk when starting a job on an authenticated print queue, which might allow local users to obtain the credentials.	unknown 2008-03-18	1.7	CVE-2008-0996 APPLE
Apple -- Mac OS X Server Apple -- Mac OS X	AppKit in Apple Mac OS X 10.4.11 inadvertently makes an NSApplication mach port available for inter-process communication instead of inter-thread communication, which allows local users to execute arbitrary code via crafted messages to provileged applications.	unknown 2008-03-18	1.9	CVE-2008-0049 APPLE
Apple -- Podcast Producer	Podcast Capture in Podcast Producer for Apple Mac OS X 10.5.2 invokes a subtask with passwords in command line arguments, which allows local users to read the passwords via process listings.	unknown 2008-03-18	2.1	CVE-2008-0993 APPLE
Apple -- Safari	WebCore, as used in Apple Safari before 3.1, does not properly mask the password field when reverse conversion is used with the Kotoeri input method, which allows physically proximate attackers to read the password.	unknown 2008-03-18	2.1	CVE-2008-1005 APPLE

Drake Team -- Drake CMS	Absolute path traversal vulnerability in install/index.php in Drake CMS 0.4.11 RC8 allows remote attackers to read and execute arbitrary files via a full pathname in the d_root parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-18	3.6	CVE-2008-1371 OTHER-REF BID
Gentoo -- Linux	The docert function in ssl-cert.eclass, when used by src_compile or src_install on Gentoo Linux, stores the SSL key in a binpkg, which (1) allows local users to extract the key from the binpkg, and (2) causes multiple systems that use this binpkg to have the same SSL key and certificate.	unknown 2008-03-18	2.1	CVE-2008-1383 OTHER-REF
Novell -- Groupwise	Unspecified vulnerability in the Windows client API in Novell GroupWise 7 before SP3 and 6.5 before SP6 Update 3 allows remote authenticated users to access the non-shared stored e-mail messages of another user who has shared at least one folder with the attacker.	unknown 2008-03-18	3.5	CVE-2008-1330 OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
RaidSonic Technology -- Firmware	RaidSonic NAS-4220-B with 2.6.0-n(2007-10-11) firmware stores a partition encryption key in an unencrypted /system/.crypt file with base64 encoding, which allows local users to obtain the key.	unknown 2008-03-20	2.1	CVE-2008-1431 BUGTRAQ BID SECUNIA
redhat -- Directory Server	Red Hat Directory Server 8.0, when running on Red Hat Enterprise Linux, uses insecure permissions for the redhat-idm-console script, which allows local users to execute arbitrary code by modifying the script.	unknown 2008-03-19	2.1	CVE-2008-0889 REDHAT

Back to top