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
FreeBSD 6.3 through 7.0	The kernel in FreeBSD 6.3 through 7.0 on amd64 platforms can make an extra swapgs call after a General Protection Fault (GPF), which allows local users to gain privileges by triggering a GPF during the kernel's return from (1) an interrupt, (2) a trap, or (3) a system call.	unknown 2008-09-05	7.2	CVE-2008-3890 FREEBSD BID
Ampache -- Ampache	gather-messages.sh in Ampache 3.4.1 allows local users to overwrite arbitrary files via a symlink attack on temporary files.	unknown 2008-09-04	7.2	CVE-2008-3929 OTHER-REF BID
anzio -- print_wizard anzio -- web_print_object	Stack-based buffer overflow in the Anzio Web Print Object (WePO) ActiveX control 3.2.19 and 3.2.24, as used in Anzio Print Wizard, allows remote attackers to execute arbitrary code via a long mainurl parameter.	unknown 2008-08-29	9.3	CVE-2008-3480 MILW0RM OTHER-REF
Aspindir -- mini_nuke_freehost	SQL injection vulnerability in members.asp in Mini-NUKE Freehost 2.3 allows remote attackers	unknown 2008-09-02	7.5	CVE-2008-3888 BUGTRAQ

	to execute arbitrary SQL commands via the uid parameter in a member_details action.			
bitlbee -- bitlbee	Unspecified vulnerability in BitlBee before 1.2.2 allows remote attackers to "recreate" and "hijack" existing accounts via unspecified vectors.	unknown 2008-09-04	7.5	CVE-2008-3920 OTHER-REF BID XF
caudium -- caudium	configvar in Caudium 1.4.12 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/roken#####.pike temporary file.	unknown 2008-09-02	7.2	CVE-2008-3883 OTHER-REF OTHER-REF BID
Cisco -- Secure ACS Cisco -- Cisco Secure Access Control Server	CSRadius.exe in Cisco Secure ACS does not properly handle an EAP Response packet in which the value of the length field exceeds the actual packet length, which allows remote attackers to cause a denial of service (service crash) or possibly execute arbitrary code via a crafted (1) EAP-Response/Identity, (2) EAP-Response/MD5, or (3) EAP-Response/TLS packet.	unknown 2008-09-04	7.5	CVE-2008-2441 BUGTRAQ
Cisco -- PIX Cisco -- adaptive_security_appliance_5500	Multiple unspecified vulnerabilities in the SIP inspection functionality in Cisco PIX and Adaptive Security Appliance (ASA) 5500 devices 7.0 before 7.0(7)16, 7.1 before 7.1(2)71, 7.2 before 7.2(4)7, 8.0 before 8.0(3)20, and 8.1 before 8.1(1)8 allow remote attackers to cause a denial of service (device reload) via unknown vectors, aka Bug IDs CSCsq07867, CSCsq57091, CSCsk60581, and CSCsq39315.	unknown 2008-09-04	7.8	CVE-2008-2732 CISCO
Cisco -- PIX Cisco -- adaptive_security_appliance_5500	Cisco PIX and Adaptive Security Appliance (ASA) 5500 devices 7.2 before 7.2(4)2, 8.0 before 8.0(3)14, and 8.1 before 8.1(1)4, when configured as a client VPN endpoint, do not properly process IPSec client authentication, which allows remote attackers to cause a denial of service (device reload) via a crafted authentication attempt, aka Bug ID CSCso69942.	unknown 2008-09-04	7.1	CVE-2008-2733 CISCO
Cisco -- adaptive_security_appliance_5500	Memory leak in the crypto functionality in Cisco Adaptive Security Appliance (ASA) 5500	unknown 2008-09-04	7.1	CVE-2008-2734 CISCO

	devices 7.2 before 7.2(4)2, 8.0 before 8.0(3)14, and 8.1 before 8.1(1)4, when configured as a clientless SSL VPN endpoint, allows remote attackers to cause a denial of service (memory consumption and VPN hang) via a crafted SSL or HTTP packet, aka Bug ID CSCso66472.			
Cisco -- adaptive_security_appliance_5500	The HTTP server in Cisco Adaptive Security Appliance (ASA) 5500 devices 8.0 before 8.0(3)15 and 8.1 before 8.1(1)5, when configured as a clientless SSL VPN endpoint, does not properly process URIs, which allows remote attackers to cause a denial of service (device reload) via a URI in a crafted SSL or HTTP packet, aka Bug ID CSCsq19369.	unknown 2008-09-04	7.1	CVE-2008-2735 CISCO
Cisco -- adaptive_security_appliance_5500	Unspecified vulnerability in Cisco Adaptive Security Appliance (ASA) 5500 devices 8.0(3)15, 8.0(3)16, 8.1(1)4, and 8.1(1)5, when configured as a clientless SSL VPN endpoint, allows remote attackers to obtain usernames and passwords via unknown vectors, aka Bug ID CSCsq45636.	unknown 2008-09-04	7.1	CVE-2008-2736 CISCO
discountedscripts -- acg_ptp	SQL injection vulnerability in index.php in ACG-PTP 1.0.6 allows remote attackers to execute arbitrary SQL commands via the adid parameter in an adorder action.	unknown 2008-09-05	7.5	CVE-2008-3944 MILW0RM BID
ezonescripts -- living_local	SQL injection vulnerability in listtest.php in eZoneScripts Living Local 1.1 allows remote attackers to execute arbitrary SQL commands via the r parameter.	unknown 2008-09-05	7.5	CVE-2008-3943 MILW0RM BID
Fedora -- directory_server redhat -- Directory Server	Red Hat Directory Server 7.1 before SP7, Red Hat Directory Server 8, and Fedora Directory Server 1.1.1 allow remote attackers to cause a denial of service (CPU consumption and search outage) via crafted LDAP search requests with patterns, related to a single-threaded regular-expression subsystem.	unknown 2008-08-29	7.1	CVE-2008-2930 OTHER-REF REDHAT SECTRACK

Fedora -- directory_server redhat -- Directory Server	Multiple memory leaks in Red Hat Directory Server 7.1 before SP7, Red Hat Directory Server 8, and Fedora Directory Server 1.1.1 and earlier allow remote attackers to cause a denial of service (memory consumption) via vectors involving (1) the authentication / bind phase and (2) anonymous LDAP search requests.	unknown 2008-08-29	7.8	CVE-2008-3283 OTHER-REF REDHAT SECTRACK
FreeBSD -- FreeBSD	sys/netinet6/icmp6.c in the kernel in FreeBSD 6.3 through 7.1 does not properly check the proposed new MTU in an ICMPv6 Packet Too Big Message, which allows remote attackers to cause a denial of service (panic) via a crafted Packet Too Big Message.	unknown 2008-09-05	7.1	CVE-2008-3530
GNU -- Ed	Heap-based buffer overflow in the strip_escapes function in signal.c in GNU ed before 1.0 allows context-dependent or user-assisted attackers to execute arbitrary code via a long filename. NOTE: since ed itself does not typically run with special privileges, this issue only crosses privilege boundaries when ed is invoked as a third-party component.	unknown 2008-09-04	9.3	CVE-2008-3916 MLIST SECTRACK XF
Google -- google_apps	The SAML Single Sign-On (SSO) Service for Google Apps allows remote service providers to impersonate users at arbitrary service providers via vectors related to authentication responses that lack a request identifier and recipient field.	unknown 2008-09-03	7.5	CVE-2008-3891 OTHER-REF CERT-VN
HP -- OpenView Network Node Manager	Unspecified vulnerability in ovalarmsrv 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-2008-3537.	unknown 2008-09-03	7.8	CVE-2008-3536
HP -- OpenView Network Node Manager	Unspecified vulnerability in ovalarmsrv in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to cause a denial of service	unknown 2008-09-03	7.8	CVE-2008-3537

	via unknown vectors, a different vulnerability than CVE-2008-3536.			
hsc -- dns2tcp	dns2tcp before 0.4.1 does not properly handle negative values in a certain length field in the input argument to the (1) dns_simple_decode or (2) dns_decode function, which allows remote attackers to overwrite a buffer and have unspecified other impact.	unknown 2008-09-04	10.0	CVE-2008-3910 MLIST OTHER-REF
justsystems -- ichitaro	Unspecified vulnerability in multiple JustSystems Ichitaro products allows remote attackers to execute arbitrary code via a crafted JTD document, as exploited in the wild in August 2008.	unknown 2008-09-04	9.3	CVE-2008-3919 OTHER-REF SECTRACK XF
Linux -- Kernel	The sbni_ioctl function in drivers/net/wan/sbni.c in the wan subsystem in the Linux kernel 2.6.26.3 does not check for the CAP_NET_ADMIN capability before processing a (1) SIOCDEVRESINSTATS, (2) SIOCDEVSHWSTATE, (3) SIOCDEVENSLAVE, or (4) SIOCDEVEMANSIPATE ioctl request, which allows local users to bypass intended capability restrictions.	unknown 2008-09-03	7.2	CVE-2008-3525 MLIST OTHER-REF
Linux -- Kernel	net/sctp/socket.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel 2.6.26.3 does not verify that the SCTP-AUTH extension is enabled before proceeding with SCTP-AUTH API functions, which allows attackers to cause a denial of service (panic) via vectors that result in calls to (1) sctp_setsockopt_auth_chunk, (2) sctp_setsockopt_hmac_ident, (3) sctp_setsockopt_auth_key, (4) sctp_setsockopt_active_key, (5) sctp_setsockopt_del_key, (6) sctp_getsockopt_maxburst, (7) sctp_getsockopt_active_key, (8) sctp_getsockopt_peer_auth_chunks, or (9) sctp_getsockopt_local_auth_chunks.	unknown 2008-09-03	7.1	CVE-2008-3792 MLIST MLIST MLIST MLIST MLIST OTHER-REF

Linux -- Kernel	The proc_do_xprt function in net/sunrpc/sysctl.c in the Linux kernel 2.6.26.3 does not check the length of a certain buffer obtained from userspace, which allows local users to overflow a stack-based buffer and have unspecified other impact via a crafted read system call for the /proc/sys/sunrpc/transports file.	unknown 2008-09-04	7.2	CVE-2008-3911 MLIST MLIST MLIST OTHER-REF
lxde -- gpicview	src/main-win.c in GPicView 0.1.9 in Lightweight X11 Desktop Environment (LXDE) allows context-dependent attackers to execute arbitrary commands via shell metacharacters in a filename.	unknown 2008-09-04	7.5	CVE-2008-3904 MLIST MLIST
Novell -- iPrint Client	Multiple heap-based buffer overflows in the IppCreateServerRef function in nipplib.dll in Novell iPrint Client 4.x before 4.38 and 5.x before 5.08 allow remote attackers to execute arbitrary code via a long argument to the (1) GetPrinterURLList, (2) GetPrinterURLList2, or (3) GetFileList2 function in the Novell iPrint ActiveX control in ienipp.ocx.	unknown 2008-09-05	9.3	CVE-2008-2436 BUGTRAQ OTHER-REF BID XF
OpenOffice -- OpenOffice.org	Integer overflow in the rtl_allocateMemory function in sal/rtl/source/alloc_global.c in the memory allocator in OpenOffice.org (OOo) 2.4.1, on 64-bit platforms, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted document, related to a "numeric truncation error," a different vulnerability than CVE-2008-2152.	unknown 2008-08-29	9.3	CVE-2008-3282 OTHER-REF OTHER-REF OTHER-REF REDHAT BID SECTRACK
ovidentia -- ovidentia	SQL injection vulnerability in index.php in Ovidentia 6.6.5 allows remote attackers to execute arbitrary SQL commands via the field parameter in a search action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-09-04	7.5	CVE-2008-3918
ozsari -- full_php_emlak_script	SQL injection vulnerability in landsee.php in Full PHP Emlak	unknown 2008-09-05	7.5	CVE-2008-3942 OTHER-REF

	Script allows remote attackers to execute arbitrary SQL commands via the id parameter.			BID
phpMyRealty -- phpMyRealty	Multiple SQL injection vulnerabilities in phpMyRealty (PMR) 1.0.9 and earlier allow remote attackers to execute arbitrary SQL commands via (1) the id parameter in pages.php and (2) the price_max parameter in search.php.	unknown 2008-08-29	7.5	CVE-2008-3861 MILW0RM BID
princeton_university -- wordnet	Multiple buffer overflows in Princeton WordNet (wn) 3.0 allow context-dependent attackers to execute arbitrary code via (1) a long argument on the command line; a long (2) WNSEARCHDIR, (3) WNHOME, or (4) WNDBVERSION environment variable; or (5) a user-supplied dictionary (aka data file). NOTE: since WordNet itself does not run with special privileges, this issue only crosses privilege boundaries when WordNet is invoked as a third party component.	unknown 2008-09-04	10.0	CVE-2008-3908 BUGTRAQ OTHER-REF XF XF XF XF
redhat -- Directory Server	Multiple buffer overflows in the adminutil library in CGI applications in Red Hat Directory Server 7.1 before SP7 allow remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted Accept-Language HTTP header.	unknown 2008-08-29	10.0	CVE-2008-2928 OTHER-REF OTHER-REF SECTRACK
ruby-lang -- Ruby	Integer overflow in the rb_ary_splice function in Ruby 1.6.x allows context-dependent attackers to trigger memory corruption via unspecified vectors, aka the "1.6.x variant" of the "REALLOC_N" variant.	unknown 2008-09-02	10.0	CVE-2008-2727 MLIST SUSE
ruby-lang -- Ruby	Integer overflow in the rb_ary_splice function in Ruby 1.6.x allows context-dependent attackers to trigger memory corruption, aka the "1.6.x variant" of the "beg + rlen" issue.	unknown 2008-09-02	10.0	CVE-2008-2728 MLIST SUSE
Source Workshop -- words_tag_script	SQL injection vulnerability in index.php in Words tag 1.2 allows remote attackers to execute arbitrary	unknown 2008-09-05	7.5	CVE-2008-3945 MILW0RM

	SQL commands via the word parameter in a claim action.			
Sun -- opensolaris Sun -- Solaris	The kernel in Sun Solaris 8 through 10 and OpenSolaris before snv_90 allows local users to bypass chroot, zones, and the Solaris Trusted Extensions multi-level security policy, and establish a covert communication channel, via unspecified vectors involving system calls.	unknown 2008-09-02	7.2	CVE-2008-3875 SUNALERT
telartis_bv -- awstats_totals	awstatstotals.php in AWStats Totals 1.0 through 1.14 allows remote attackers to execute arbitrary code via PHP sequences in the sort parameter, which is used by the multisort function when dynamically creating an anonymous PHP function.	unknown 2008-09-04	9.3	CVE-2008-3922 BUGTRAQ OTHER-REF XF
tiger -- tiger	genmsgidx in Tiger 3.2.2 allows local users to overwrite or delete arbitrary files via a symlink attack on temporary files.	unknown 2008-09-04	7.2	CVE-2008-3927 OTHER-REF
ultrashareware -- ultra_office_control	Stack-based buffer overflow in the Ultra.OfficeControl ActiveX control in OfficeCtrl.ocx 2.0.2008.801 in Ultra Shareware Ultra Office Control allows remote attackers to execute arbitrary code via long strUrl, strFile, and strPostData parameters to the HttpUpload method.	unknown 2008-09-02	9.3	CVE-2008-3878 MILW0RM OTHER-REF OTHER-REF BID
ultrashareware -- ultra_office_control	The Ultra.OfficeControl ActiveX control in OfficeCtrl.ocx 2.0.2008.801 and earlier in Ultra Shareware Ultra Office Control allows remote attackers to force the download of arbitrary files onto a client system via a URL in the first argument to the Open method, in conjunction with a full destination pathname in the first argument (SaveAsDocument argument) to the Save method.	unknown 2008-09-02	9.3	CVE-2008-3879 MILW0RM OTHER-REF OTHER-REF BID
VMWare -- VMWare Player VMWare -- VMware Server VMWare -- VMWare Workstation VMWare -- ACE	Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, VMware	unknown 2008-09-03	10.0	CVE-2008-3691 BUGTRAQ FULLDISC OTHER-REF OTHER-REF

	Player 1.x before 1.0.8 build 108000, VMware Player 2.x before 2.0.5 build 109488, VMware ACE 1.x before 1.0.7 build 108880, VMware ACE 2.x before 2.0.5 build 109488, and VMware Server before 1.0.7 build 108231 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-3692, CVE-2008-3693, CVE-2008-3694, CVE-2008-3695, and CVE-2008-3696.			OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
VMWare -- VMWare Player VMWare -- VMware Server VMWare -- VMWare Workstation VMWare -- ACE	Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, VMware Player 1.x before 1.0.8 build 108000, VMware Player 2.x before 2.0.5 build 109488, VMware ACE 1.x before 1.0.7 build 108880, VMware ACE 2.x before 2.0.5 build 109488, and VMware Server before 1.0.7 build 108231 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-3691, CVE-2008-3693, CVE-2008-3694, CVE-2008-3695, and CVE-2008-3696.	unknown 2008-09-03	10.0	CVE-2008-3692 BUGTRAQ FULLDISC OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
VMWare -- VMWare Player VMWare -- VMware Server VMWare -- VMWare Workstation VMWare -- ACE	Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, VMware Player 1.x before 1.0.8 build 108000, VMware Player 2.x before 2.0.5 build 109488, VMware ACE 1.x before 1.0.7 build 108880, VMware ACE 2.x before 2.0.5 build 109488, and VMware Server before 1.0.7 build 108231 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-3691, CVE-2008-3692, CVE-2008-3694, CVE-2008-3695, and CVE-2008-3696.	unknown 2008-09-03	10.0	CVE-2008-3693 BUGTRAQ FULLDISC OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
VMWare -- VMWare Player VMWare -- VMware Server VMWare -- VMWare Workstation VMWare -- ACE	Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x	unknown 2008-09-03	10.0	CVE-2008-3694 BUGTRAQ FULLDISC OTHER-REF

	before 6.0.5 build 109488, VMware Player 1.x before 1.0.8 build 108000, VMware Player 2.x before 2.0.5 build 109488, VMware ACE 1.x before 1.0.7 build 108880, VMware ACE 2.x before 2.0.5 build 109488, and VMware Server before 1.0.7 build 108231 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-3691, CVE-2008-3692, CVE-2008-3693, CVE-2008-3695, and CVE-2008-3696.			OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
VMWare -- VMWare Player VMWare -- VMware Server VMWare -- VMWare Workstation VMWare -- ACE	Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, VMware Player 1.x before 1.0.8 build 108000, VMware Player 2.x before 2.0.5 build 109488, VMware ACE 1.x before 1.0.7 build 108880, VMware ACE 2.x before 2.0.5 build 109488, and VMware Server before 1.0.7 build 108231 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-3691, CVE-2008-3692, CVE-2008-3693, CVE-2008-3694, and CVE-2008-3696.	unknown 2008-09-03	10.0	CVE-2008-3695 BUGTRAQ FULLDISC OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
VMWare -- VMWare Player VMWare -- VMware Server VMWare -- VMWare Workstation VMWare -- ACE	Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, VMware Player 1.x before 1.0.8 build 108000, VMware Player 2.x before 2.0.5 build 109488, VMware ACE 1.x before 1.0.7 build 108880, VMware ACE 2.x before 2.0.5 build 109488, and VMware Server before 1.0.7 build 108231 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-3691, CVE-2008-3692, CVE-2008-3693, CVE-2008-3694, and CVE-2008-3695.	unknown 2008-09-03	10.0	CVE-2008-3696 BUGTRAQ FULLDISC OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
VMWare -- VMWare Player VMWare -- VMware Server VMWare -- VMWare Workstation	Unspecified vulnerability in the OpenProcess function in VMware Workstation 5.5.x before 5.5.8 build	unknown 2008-09-03	7.2	CVE-2008-3698 BUGTRAQ FULLDISC

VMWare -- ACE	108000, VMware Workstation 6.0.x before 6.0.5 build 109488, VMware Player 1.x before 1.0.8 build 108000, VMware Player 2.x before 2.0.5 build 109488, VMware ACE 1.x before 1.0.7 build 108880, VMware ACE 2.x before 2.0.5 build 109488, and VMware Server before 1.0.7 build 108231 on Windows allows local host OS users to gain privileges on the host OS via unknown vectors.			OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECUNIA
VMWare -- VMWare Player VMWare -- VMware Server VMWare -- VMWare Workstation VMWare -- ACE	Buffer overflow in a certain ActiveX control in the COM API in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, VMware Player 1.x before 1.0.8 build 108000, VMware Player 2.x before 2.0.5 build 109488, VMware ACE 1.x before 1.0.7 build 108880, VMware ACE 2.x before 2.0.5 build 109488, and VMware Server before 1.0.7 build 108231 allows remote attackers to cause a denial of service (browser crash) or possibly execute arbitrary code via a call to the GuestInfo method in which there is a long string argument, and an assignment of a long string value to the result of this call. NOTE: this may overlap CVE-2008-3691, CVE-2008-3692, CVE-2008-3693, CVE-2008-3694, CVE-2008-3695, or CVE-2008-3696.	unknown 2008-09-03	10.0	CVE-2008-3892 BUGTRAQ FULLDISC MILW0RM OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
Wireshark -- Wireshark Ethereal Group -- Ethereal	Unspecified vulnerability in Wireshark and Ethereal on SUSE Linux allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors.	unknown 2008-09-02	8.3	CVE-2008-3146 SUSE
XMLSoft -- Libxml2	libxml2, possibly before 2.5.0, does not properly detect recursion during entity expansion, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references,	unknown 2008-09-02	7.1	CVE-2008-3538 MLIST OTHER-REF OTHER-REF

	aka the "billion laughs attack."			
zoneminder -- zoneminder	SQL injection vulnerability in zm_html_view_event.php in ZoneMinder 1.23.3 and earlier allows remote attackers to execute arbitrary SQL commands via the filter array parameter.	unknown 2008-09-02	7.5	CVE-2008-3880 BUGTRAQ BID XF
zoneminder -- zoneminder	ZoneMinder 1.23.3 and earlier allows remote attackers to execute arbitrary commands (aka "Command Injection") via (1) the executeFilter function in zm_html_view_events.php and (2) the run_state parameter to zm_html_view_state.php.	unknown 2008-09-02	10.0	CVE-2008-3882 BUGTRAQ BID XF

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Acoustica -- mixcraft	Stack-based buffer overflow in Acoustica Mixcraft 4.1 Build 96 and 4.2 Build 98 allows user-assisted attackers to execute arbitrary code via a crafted .mx4 file.	unknown 2008-09-02	6.8	CVE-2008-3877 MILW0RM BID
Adobe -- Flash Player	The System.setClipboard method in Adobe Flash Player allows remote attackers to populate the clipboard with a URL that is difficult to delete, as exploited in the wild in August 2008.	unknown 2008-08-29	4.3	CVE-2008-3873 OTHER-REF OTHER-REF OTHER-REF SECTRACK
Apple -- Quicktime	Apple QuickTime before 7.4.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted ftyp atoms in a movie file, which triggers memory corruption.	unknown 2008-09-03	6.8	CVE-2008-1739 OTHER-REF
avtech -- pager_enterprise	Directory traversal vulnerability in the web interface in AVTECH PageR Enterprise before 5.0.7 allows remote attackers to read arbitrary files via directory traversal sequences in the URI.	unknown 2008-09-05	5.0	CVE-2008-3939 FULLDISC BID

bizdirectory -- bizdirectory	Cross-site scripting (XSS) vulnerability in BizDirectory 2.04 and earlier allows remote attackers to inject arbitrary web script or HTML via the page parameter in a search action to the default URI.	unknown 2008-09-05	4.3	CVE-2008-3941 BUGTRAQ BID
Blogn -- Blogn	Cross-site scripting (XSS) vulnerability in Blogn (BURO GUN) 1.9.7 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different issue than CVE-2006-6176.	unknown 2008-09-02	4.3	CVE-2008-3884 OTHER-REF
Blogn -- Blogn	Cross-site request forgery (CSRF) vulnerability in Blogn (BURO GUN) 1.9.7 and earlier allows remote attackers to make content modifications as arbitrary users via unspecified vectors. NOTE: some of these details are obtained from third party information.	unknown 2008-09-02	6.8	CVE-2008-3885 OTHER-REF IPA-JPCERT
Clam Anti-Virus -- ClamAV	libclamav/chmunpack.c in the chm-parser in ClamAV before 0.94 allows remote attackers to cause a denial of service (application crash) via a malformed CHM file, related to an "invalid memory access."	unknown 2008-09-04	5.0	CVE-2008-1389 OTHER-REF OTHER-REF OTHER-REF
d-ic -- shop_v52 d-ic -- shop_v50	Cross-site scripting (XSS) vulnerability in DIC shop_v50 3.0 and earlier and shop_v52 2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-09-05	4.3	CVE-2008-3935 BID IPA-JPCERT
davlin -- thickbox_gallery	Davlin Thickbox Gallery 2 allows remote attackers to obtain the administrative username and MD5 password hash via a direct request to conf/admins.php.	unknown 2008-08-29	5.0	CVE-2008-3859 MILW0RM XF
Debian -- honeyd_common	test.sh in Honeyd 1.5c might allow local users to overwrite arbitrary files via a symlink attack on temporary files.	unknown 2008-09-04	6.9	CVE-2008-3928 OTHER-REF

Debian -- citadel_server	migrate_aliases.sh in Citadel Server 7.37 allows local users to overwrite arbitrary files via a symlink attack on temporary files.	unknown 2008-09-04	6.9	CVE-2008-3930 OTHER-REF
Django Project -- Django	The administration application in Django 0.91, 0.95, and 0.96 stores unauthenticated HTTP POST requests and processes them after successful authentication occurs, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks and delete or modify data via unspecified requests.	unknown 2008-09-04	4.3	CVE-2008-3909 MLIST
dotProject -- dotProject	Multiple cross-site scripting (XSS) vulnerabilities in index.php in dotProject 2.1.2 allow remote attackers to inject arbitrary web script or HTML via (1) the inactive parameter in a tasks action, (2) the date parameter in a calendar day_view action, (3) the callback parameter in a public calendar action, or (4) the type parameter in a ticketsmith action.	unknown 2008-09-02	4.3	CVE-2008-3886 OTHER-REF
dotProject -- dotProject	Multiple SQL injection vulnerabilities in index.php in dotProject 2.1.2 allow (1) remote authenticated users to execute arbitrary SQL commands via the tab parameter in a projects action, and (2) remote authenticated administrators to execute arbitrary SQL commands via the user_id parameter in a viewuser action.	unknown 2008-09-02	6.0	CVE-2008-3887 OTHER-REF
Dreambox -- DM500C	The web interface in Dreambox DM500C allows remote attackers to cause a denial of service (application hang) via a long URI.	unknown 2008-09-05	5.0	CVE-2008-3936 BUGTRAQ FULLDISC OTHER-REF SECTRACK
Fedora -- directory_server redhat -- Directory Server	Multiple cross-site scripting (XSS) vulnerabilities in the adminutil library in the	unknown 2008-08-29	4.3	CVE-2008-2929 OTHER-REF REDHAT

	Directory Server Administration Express and Directory Server Gateway (DSGW) web interface in Red Hat Directory Server 7.1 before SP7 and 8 EL4 and EL5, and Fedora Directory Server, allow remote attackers to inject arbitrary web script or HTML via input values that use % (percent) escaping.			REDHAT SECTRACK
FreeBSD -- FreeBSD	Stack-based buffer overflow in sys/kern/vfs_mount.c in the kernel in FreeBSD 7.0 and 7.1, when vfs.usermount is enabled, allows local users to gain privileges via a crafted (1) mount or (2) nmount system call, related to copying of "user defined data" in "certain error conditions."	unknown 2008-09-05	6.9	CVE-2008-3531 FREEBSD
hans_oesterholt -- cmme	Multiple cross-site scripting (XSS) vulnerabilities in statistics.php in Content Management Made Easy (CMME) 1.12 allow remote attackers to inject arbitrary web script or HTML via the (1) page and (2) year parameters in an hstat_year action.	unknown 2008-09-04	4.3	CVE-2008-3923 MILW0RM BID XF
hans_oesterholt -- cmme	The "Make a backup" functionality in Content Management Made Easy (CMME) 1.12 stores sensitive information under the web root with insufficient access control, which allows remote attackers to discover (1) account names and (2) password hashes via a direct request for (a) backup/cmme_data.zip or (b) backup/cmme_cmme.zip.	unknown 2008-09-04	4.3	CVE-2008-3924 MILW0RM BID XF
hans_oesterholt -- cmme	Cross-site request forgery (CSRF) vulnerability in admin.php in Content Management Made Easy (CMME) 1.12 allows remote attackers to trigger the logout	unknown 2008-09-04	4.3	CVE-2008-3925 MILW0RM XF

	of an administrative user via a logout action.			
hans_oesterholt -- cmme	Multiple directory traversal vulnerabilities in Content Management Made Easy (CMME) 1.12 allow remote attackers to (1) read arbitrary files via a .. (dot dot) in the env parameter in a weblog action to index.php, or (2) create arbitrary directories via a .. (dot dot) in the env parameter in a login action to admin.php.	unknown 2008-09-04	5.8	CVE-2008-3926 MILW0RM BID XF
HP -- OpenVMS	Format string vulnerability in the finger client in HP TCP/IP Services for OpenVMS 5.x allows local users to gain privileges via format string specifiers in a (1) .plan or (2) .project file.	unknown 2008-09-05	4.4	CVE-2008-3940 OTHER-REF BID
IBM -- Lotus Quickr	Multiple cross-site scripting (XSS) vulnerabilities (1) in the WYSIWYG editors, (2) during local group creation, (3) during HTML redirects, (4) in the HTML import, (5) in the Rich text editor, and (6) in link-page in IBM Lotus Quickr 8.1 services for Lotus Domino before Hotfix 15 allow remote attackers to inject arbitrary web script or HTML via unknown vectors, including (7) the Imported Page. NOTE: the vulnerability in the WYSIWYG editors may exist because of an incomplete fix for CVE-2008-2163.	unknown 2008-08-29	4.3	CVE-2008-3860 OTHER-REF SECTRACK XF
Linksys -- WRT350N Atheros -- ar5416-ac1e_chipset	The driver for the Linksys WRT350N Wi-Fi access point with firmware 2.00.17 on the Atheros AR5416-AC1E chipset does not properly parse the Atheros vendor-specific information element in an association request, which allows remote authenticated users to cause a denial of service (device reboot or hang)	unknown 2008-09-05	6.3	CVE-2007-5474 BUGTRAQ BID

	or possibly execute arbitrary code via an Atheros information element with an invalid length, as demonstrated by an element that is too long.			
Linux -- Kernel	fs/direct-io.c in the dio subsystem in the Linux kernel before 2.6.23 does not properly zero out the dio struct, which allows local users to cause a denial of service (OOPS), as demonstrated by a certain fio test.	unknown 2008-09-04	4.7	CVE-2007-6716 MLIST MLIST OTHER-REF OTHER-REF
lxde -- lightweight_x11_desktop_environment	src/main-win.c in GPicView 0.1.9 in Lightweight X11 Desktop Environment (LXDE) allows local users to overwrite arbitrary files via a symlink attack on the /tmp/rot.jpg temporary file.	unknown 2008-09-03	4.6	CVE-2008-3791 MLIST MLIST MLIST OTHER-REF
Mono Project -- Mono	CRLF injection vulnerability in Sys.Web in Mono 2.0 and earlier allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via CRLF sequences in the query string.	unknown 2008-09-04	4.3	CVE-2008-3906 MLIST OTHER-REF BID
NetGear -- wn802t marvell -- 88w8361w-bem1	The Marvell driver for the Netgear WN802T Wi-Fi access point with firmware 1.3.16 on the Marvell 88W8361P-BEM1 chipset does not properly parse EAPoL-Key packets, which allows remote authenticated users to cause a denial of service (device reboot or hang) or possibly execute arbitrary code via a malformed EAPoL-Key packet with a crafted "advertised length."	unknown 2008-09-05	6.3	CVE-2008-1144 BUGTRAQ BID
NetGear -- wn802t marvell -- 88w8361w-bem1	The Marvell driver for the Netgear WN802T Wi-Fi access point with firmware 1.3.16 on the Marvell 88W8361P-BEM1 chipset	unknown 2008-09-05	6.3	CVE-2008-1197 BUGTRAQ BID

	does not properly parse the SSID information element in an association request, which allows remote authenticated users to cause a denial of service (device reboot or hang) or possibly execute arbitrary code via a "Null SSID."			
newsbeuter -- newsbeuter	The open-in-browser command in newsbeuter before 1.1 allows remote attackers to execute arbitrary commands via shell metacharacters in a feed URL.	unknown 2008-09-04	6.8	CVE-2008-3907 MLIST OTHER-REF BID
opendb -- OpenDb	Multiple cross-site scripting (XSS) vulnerabilities in Open Media Collectors Database (OpenDb) 1.0.6 allow remote attackers to inject arbitrary web script or HTML via the (1) user_id parameter in an edit action to user_admin.php, the (2) title parameter to listings.php, and the (3) redirect_url parameter to user_profile.php.	unknown 2008-09-05	4.3	CVE-2008-3937 OTHER-REF BID
opendb -- OpenDb	Cross-site request forgery (CSRF) vulnerability in user_admin.php in Open Media Collectors Database (OpenDb) 1.0.6 allows remote attackers to change arbitrary passwords via an update_password action.	unknown 2008-09-05	5.8	CVE-2008-3938 OTHER-REF
ovidentia -- ovidentia	Cross-site scripting (XSS) vulnerability in index.php in Ovidentia 6.6.5 allows remote attackers to inject arbitrary web script or HTML via the field parameter in a search action.	unknown 2008-09-04	4.3	CVE-2008-3917 BUGTRAQ BID
r_foundation -- r	javareconf in R 2.7.2 allows local users to overwrite arbitrary files via a symlink attack on temporary files.	unknown 2008-09-04	6.9	CVE-2008-3931 OTHER-REF
ruby-lang -- Ruby	resolv.rb in Ruby 1.8.5 and earlier, 1.8.6 before 1.8.6-p287, 1.8.7 before 1.8.7-p72, and 1.9 r18423 and	unknown 2008-09-04	5.8	CVE-2008-3905 MLIST MLIST

	earlier uses sequential transaction IDs and constant source ports for DNS requests, which makes it easier for remote attackers to spoof DNS responses, a different vulnerability than CVE-2008-1447.			
telartis_bv -- awstats_totals	Multiple cross-site scripting (XSS) vulnerabilities in AWStats Totals 1.0 through 1.14 allow remote attackers to inject arbitrary web script or HTML via the (1) month and (2) year parameter.	unknown 2008-09-04	4.3	CVE-2008-3921 BUGTRAQ OTHER-REF XF
VMWare -- VMware Server	An unspecified ISAPI extension in VMware Server before 1.0.7 build 108231 allows remote attackers to cause a denial of service (IIS crash) via a malformed request.	unknown 2008-09-03	5.0	CVE-2008-3697 BUGTRAQ FULLDISC OTHER-REF BID
vtiger -- vtiger_crm	Multiple cross-site scripting (XSS) vulnerabilities in vtiger CRM 5.0.4 allow remote attackers to inject arbitrary web script or HTML via (1) the parenttab parameter in an index action to the Products module, as reachable through index.php; (2) the user_password parameter in an Authenticate action to the Users module, as reachable through index.php; or (3) the query_string parameter in a UnifiedSearch action to the Home module, as reachable through index.php.	unknown 2008-09-03	4.3	CVE-2008-3101 BUGTRAQ OTHER-REF OTHER-REF FRSIRT XF
xrms -- xrms_crm	Multiple cross-site scripting (XSS) vulnerabilities in XRMS allow remote attackers to inject arbitrary web script or HTML via (1) the real name field, related to the user list; (2) the target parameter to login.php, (3) the title parameter to activities/some.php, (4) the company_name parameter to	unknown 2008-09-05	4.3	CVE-2008-3664 BUGTRAQ BID

	companies/some.php, (5) the last_name parameter to contacts/some.php, (6) the campaign_title parameter to campaigns/some.php, (7) the opportunity_title parameter to opportunities/some.php, (8) the case_title parameter to cases/some.php, (9) the file_id parameter to files/some.php, or (10) the starting parameter to reports/custom/mileage.php, a related issue to CVE-2008-1129.			
zoneminder -- zoneminder	Multiple cross-site scripting (XSS) vulnerabilities in ZoneMinder 1.23.3 and earlier allow remote attackers to inject arbitrary web script or HTML via unspecified parameters to unspecified "zm_html_view_*.php" files.	unknown 2008-09-02	4.3	CVE-2008-3881 BUGTRAQ BID XF

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Apple -- iPhone	Apple iPhone 2.0.2, in some configurations, allows physically proximate attackers to bypass intended access restrictions, and obtain sensitive information or make arbitrary use of the device, via an Emergency Call tap and a Home double-tap, followed by a tap of any contact's blue arrow.	unknown 2008-09-02	1.9	CVE-2008-3876 OTHER-REF SECTRACK
Asterisk -- p_b_x trixbox -- pbx	Asterisk PBX 1.2 through 1.6 and Trixbox PBX 2.6.1, when running with Digest authentication and authalwaysreject enabled, generates different responses depending on whether or not a SIP username is valid, which allows remote attackers to enumerate valid usernames.	unknown 2008-09-04	3.5	CVE-2008-3903 OTHER-REF
freed0m -- disckcryptor	DiskCryptor 0.2.6 on Windows stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer before and after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.	unknown 2008-09-03	2.1	CVE-2008-3897 BUGTRAQ OTHER-REF OTHER-REF

GNU -- grub_legacy	Grub Legacy 0.97 and earlier stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer before and after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.	unknown 2008-09-03	2.1	CVE-2008-3896 BUGTRAQ OTHER-REF OTHER-REF
HP -- 68dtt	HP firmware 68DTT F.0D stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer, aka SSRT080104.	unknown 2008-09-03	2.1	CVE-2008-3902 BUGTRAQ OTHER-REF OTHER-REF
IBM -- lenovo_7cetb5ww	IBM Lenovo firmware 7CETB5WW 2.05 stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.	unknown 2008-09-03	2.1	CVE-2008-3894 BUGTRAQ OTHER-REF OTHER-REF
Intel -- bios	Intel firmware PE94510M.86A.0050.2007.0710.1559 stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.	unknown 2008-09-03	2.1	CVE-2008-3900 BUGTRAQ OTHER-REF OTHER-REF SECTRACK
lilo -- lilo	LILO 22.6.1 and earlier stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer before and after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.	unknown 2008-09-03	2.1	CVE-2008-3895 BUGTRAQ OTHER-REF OTHER-REF
Lussumo -- Vanilla	Cross-site scripting (XSS) vulnerability in account.php in Lussumo Vanilla 1.1.5-rc1, 1.1.4, and earlier allows remote authenticated users to inject arbitrary web script or HTML via the Value field (aka Label ==> Value pairs). NOTE: some of these details are obtained from third party information.	unknown 2008-08-29	3.5	CVE-2008-3874 OTHER-REF OTHER-REF OTHER-REF BID
Microsoft -- windows-nt	Microsoft Bitlocker in Windows Vista before SP1 stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer during boot, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.	unknown 2008-09-03	1.9	CVE-2008-3893 OTHER-REF SECUNIA
secustar -- drivecrypt_plus_pack	Secu Star DriveCrypt Plus Pack 3.9 stores pre-boot authentication passwords in the BIOS	unknown 2008-09-03	2.1	CVE-2008-3898 BUGTRAQ

	Keyboard buffer and does not clear this buffer before and after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.			OTHER-REF OTHER-REF
suspend2 -- software_suspend_2	Software suspend 2 2-2.2.1, when used with the Linux kernel 2.6.16, stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.	unknown 2008-09-03	2.1	CVE-2008-3901 OTHER-REF
TrueCrypt Foundation -- TrueCrypt	TrueCrypt 5.0 stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer before and after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer. NOTE: the researcher mentions a response from the vendor denying the vulnerability.	unknown 2008-09-03	2.1	CVE-2008-3899 BUGTRAQ OTHER-REF OTHER-REF
VMWare -- esx	The VMware Consolidated Backup (VCB) command-line utilities in VMware ESX 3.0.1 through 3.0.3 and ESX 3.5 place a password on the command line, which allows local users to obtain sensitive information by listing the process.	unknown 2008-09-03	2.1	CVE-2008-2101 BUGTRAQ FULLDISC BID
Wireshark -- Wireshark	Wireshark (formerly Ethereal) 0.9.7 through 1.0.2 allows attackers to cause a denial of service (hang) via a crafted NCP packet that triggers an infinite loop.	unknown 2008-09-04	3.3	CVE-2008-3932 OTHER-REF
Wireshark -- Wireshark	Wireshark (formerly Ethereal) 0.10.14 through 1.0.2 allows attackers to cause a denial of service (crash) via a packet with crafted zlib-compressed data that triggers an invalid read in the tvb_uncompress function.	unknown 2008-09-04	3.3	CVE-2008-3933 OTHER-REF OTHER-REF
Wireshark -- Wireshark	Unspecified vulnerability in Wireshark (formerly Ethereal) 0.99.6 through 1.0.2 allows attackers to cause a denial of service (crash) via a crafted Tektronix .rf5 file.	unknown 2008-09-04	3.3	CVE-2008-3934

Back to top