Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Microsoft DirectX DirectShow 7.0 to 9.0c	A buffer overflow vulnerability has been reported in DirectX DirectShow that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-050.mspx Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf **V1.3 Updated to note availability of Microsoft Knowledge Base Article 909596 and to clarify an issue affecting Windows 2000 SP4 customers, also updates of file versions.** Currently we are not aware of any exploits for this vulnerability.	Microsoft DirectX DirectShow Arbitrary Code Execution CVE-2005-2128	High	Microsoft, Security Bulletin MS05-050, October 11, 2005 USCERT, VU#995220 Technical Cyber Security Alert TA05-284A, October 11, 2005 Avaya, ASA-2005-214, October 11, 2005 **Microsoft, Security Bulletin MS05-050 V1.3, October 21, 2005**
Microsoft Microsoft Internet Explorer 6.0 SP2	A vulnerability has been reported in Internet Explorer, J2SE Runtime Environment, that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Microsoft Internet Explorer Denial of Service	Low	Security Tracker, Alert ID: 1015101, October 25, 2005
Microsoft Network Connection Manager	A vulnerability has been reported in Network Connection Manager that could let malicious users cause a Denial of Service. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-045.mspx **V1.1 Updated to revise the install registry key name.** An exploit has been published.	Microsoft Network Connection Manager Denial of Service CAN-2005-2307	Low	Microsoft Security Bulletin MS05-045, October 11, 2005 **Microsoft Security Bulletin MS05-045 V1.1, October 21, 2005**
Microsoft Windows Plug and Play	A buffer overflow vulnerability has been reported in Windows Plug and Play that could let malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-047.mspx Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf **An exploit has been published.**	Microsoft Windows Plug and Play Arbitrary Code Execution CVE-2005-2120	High	Microsoft, Security Bulletin MS05-047, October 11, 2005 USCERT, VU#214572 Technical Cyber Security Alert TA05-284A, October 11, 2005 Avaya, ASA-2005-214, October 11, 2005 **Security Focus, ID: 15065, October 24, 2005**
RSA RSA ACE/ Agent for Web 5.1, Authentication for Web 5.1, 5.2, 5.3	A vulnerability has been reported in RSA ACE/ Agent for Web and Authentication Agent for Web that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	RSA ACE/ Agent for Web Cross-Site Scripting CVE-2005-3329	Medium	Security Focus, ID: 15206, October 26, 2005
Symantec Symantec Discovery 6.0, Standard 4.5.X, Web 4.5.X	A vulnerability has been reported in Symantec Discovery that could let remote malicious users obtain unauthorized access. Vendor fix available: http://securityresponse.symantec.com/avcenter/security/Content/2005.10.24.html There is no exploit code required.	Symantec Discovery Unauthorized Access CVE-2005-3316	Medium	Symantec, Security Response SYM05-022, October 24, 2005

Veritas NetBackup Data and Business Center 4.5FP, 4.5MP, Client/ Enterprise/ Server 5.0, 5.1, 6.0	A vulnerability has been reported in NetBackup that could let remote malicious users execute arbitrary code. Vendor fix available: http://seer.support.veritas.com/docs/279085.htm **An exploit has been published.**	VERITAS NetBackup Arbitrary Code Execution CVE-2005-2715	High	Secunia, Advisory: SA17181, October 13, 2005 USCERT, VU#495556 **Security Focus, ID: 15079, October 20, 2005**
ZipGenius prior to 6.0.2.1050	A buffer overflow vulnerability has been reported in ZipGenius, ACE, ZIP, and UUE processing, that could let remote malicious users execute arbitrary code. Upgrade to version 6.0.2.1050: http://downloads.zipgenius.it/zipgenius/index.htm Currently we are not aware of any exploits for this vulnerability.	ZipGenius Arbitrary Code Execution CVE-2005-3317	High	Security Tracker, Alert ID: 1015090, October 21, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Apache Software Foundation Apache 2.0.x	A vulnerability has been reported in 'modules/ssl/ssl_engine_kernel.c' because the 'ssl_hook_Access()' function does not properly enforce the 'SSLVerifyClient require' directive in a per-location context if a virtual host is configured with the 'SSLVerifyCLient optional' directive, which could let a remote malicious user bypass security policies. Patch available at: http://svn.apache.org/viewcvs?rev=264800&view=rev OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Debian: http://security.debian.org/pool/updates/main/a/apache2/ Mandriva: http://www.mandriva.com/security/advisories Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/liba/ Gentoo:	Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass CVE-2005-2700	Medium	Security Tracker Alert ID: 1014833, September 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.017, September 3, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Debian Security Advisory, DSA 805-1, September 8, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005 Slackware Security Advisory, SSA:2005-251-02, September 9, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 Debian Security Advisory DSA 807-1, September 12, 2005 US-CERT VU#744929 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 Avaya Security Advisory, ASA-2005-204, September 23, 2005 Conectiva Linux Announcement, CLSA-2005:1013,

	http://security.gentoo.org/glsa/glsa-200509-12.xml Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-204.pdf Conectiva: ftp://atualizacoes.conectiva.com.br/10/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ HP: http://software.hp.com/ **Trustix:** **http://http.trustix.org/pub/trustix/updates/** There is no exploit code required.			September 27, 2005 Turbolinux Security Advisory, TLSA-2005-94, October 3, 2005 HP Security Bulletin, HPSBUX-01232, October 5, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005**
BMC Software Control-M Agent 6.1.03	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user overwrite files. No workaround or patch available at time of publishing. There is no exploit code required.	BMC Control-M Agent Insecure File Permission CVE-2005-3311	Medium	Security Focus, Bugtraq ID: 15167, October 22, 2005
Clam Anti-Virus ClamAV 0.80 -0.86.2, 0.70, 0.65-0.68, 0.60, 0.51-0.54	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'libclamav/upx.c' due to a signedness error, which could let a malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported in 'libclamav/fsg.c' when handling a specially -crafted FSG-compressed executable file. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=86638 Gentoo: http://security.gentoo.org/glsa/glsa-200509-13.xml Mandriva: http://www.mandriva.com/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/c/clamav/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Currently we are not aware of any exploits for these vulnerabilities.	ClamAV UPX Buffer Overflow & FSG Handling Denial of Service CVE-2005-2919 CVE-2005-2920	High	Secunia Advisory: SA16848, September 19, 2005 Gentoo Linux Security Advisory, GLSA 200509-13, September 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:166, September 20, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0051, September 23, 2005 Debian Security Advisory DSA 824-1, September 29, 2005 Conectiva Linux Announcement, CLSA-2005:1020, October 3, 2005 **US-CERT VU#363713**
DCP-Portal DCP-Portal 6.1.1, 6.1, 6.0 5.3-5.3.2, 5.2, 5.1, 5.0.2, 5.0.1, 4.5.1, 4.2, 4.1, 4.0, 3.7	Several Cross-Site Scripting and SQL Injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML, script code and SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	DCP-Portal Cross-Site Scripting & SQL Injection	Medium	Security Focus, Bugtraq ID: 15183, October 24, 2005

Debian module-assistant	A vulnerability has been reported in module-assist due to the insecure creation of temporary files, which could let a malicious user overwrite files. Update available at: http://security.debian.org/pool/updates/main/m/module-assistant/ There is no exploit code required.	Debian Module-Assistant Insecure Temporary File Creation CVE-2005-3121	Medium	Debian Security Advisory DSA 867-1, October 20, 2005
Detlev Offenbach eric3 prior to 3.7.2	A vulnerability has been reported due to a "potential security exploit." The impact was not specified Upgrades available at: http://prdownloads.sourceforge.net/eric-ide/eric-3.7.2.tar.gz?download **Debian:** **http://security.debian.org/pool/updates/main/e/eric/** Currently we are not aware of any exploits for this vulnerability.	eric3 Unspecified Vulnerability CVE-2005-3068	Not Specified	Security Tracker Alert ID: 1014947, September 21, 2005 **Debian Security Advisory, DSA 869-1, October 21, 2005**
Eric S Raymond Fetchmail 6.x	A vulnerability has been reported in the 'fetchmailconf' configuration utility due to a race condition, which could let a malicious user obtain sensitive information. Upgrades available at: http://download.berlios.de/fetchmail/ There is no exploit code required.	Fetchmail 'fetchmailconf' Information Disclosure CVE-2005-3088	Medium	fetchmail-SA-2005-02 Security Announcement, October 21, 2005

Glyph and Cog XPDF prior to 3.00pl3	A buffer overflow vulnerability exists in ' 'xpdf/Decrypt.cc' due to a boundary error in the 'Decrypt::makeFileKey2' function, which could let a remote malicious user execute arbitrary code. Update available at: http://www.foolabs.com/xpdf/download.html Patch available at: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch Debian: http://security.debian.org/pool/updates/main/c/cupsys/ http://security.debian.org/pool/updates/main/x/xpdf/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/ KDE: ftp://ftp.kde.org/pub/kde/security_patches Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.suse.com/pub/suse/ FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-10.xml SGI: ftp://patches.sgi.com/support/free/security/advisories/ Trustix: http://http.trustix.org/pub/trustix/updates/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-026.html **SCO: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.42/600**	Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow CVE-2005-0064	High	iDEFENSE Security Advisory, January 18, 2005 Conectiva Linux Security Announcement, CLA-2005:921, January 25, 2005 Mandrakelinux Security Update Advisories, MDKSA-2005:016-021, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 SGI Security Advisory, 20050202-01-U, February 9, 2005 Gentoo Linux Security Advisory, GLSA 200502-10, February 9, 2005 Fedora Legacy Update Advisory, FLSA:2353, February 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003, February 11, 2005 Fedora Legacy Update Advisory, FLSA:2127, March 2, 2005 SUSE Security Announcement, SUSE-SA:2005:015, March 14, 2005 RedHat Security Advisory, RHSA-2005:026-15, March 16, 2005 SuSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005 **SCO Security Advisory, SCOSA-2005.42, October 20, 2005**

	Currently we are not aware of any exploits for this vulnerability.			
GNU Texinfo 4.7	A vulnerability has been reported in 'textindex.c' due to insecure creation of temporary files by the 'sort_offline()' function, which could let a malicious user create/ overwrite arbitrary files. Gentoo: http://security.gentoo.org/glsa/glsa-200510-04.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/texinfo/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Trustix:** **http://http.trustix.org/pub/trustix/updates/** There is no exploit code required.	GNU Texinfo Insecure Temporary File Creation CVE-2005-3011	Medium	Security Focus, Bugtraq ID: 14854, September 15, 2005 Gentoo Linux Security Advisory, GLSA 200510-04, October 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:175, October 6, 2005 Ubuntu Security Notice, USN-194-1, October 06, 2005 SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005**
GNU Xpdf prior to 3.00pl2	A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code on the target user's system. A remote user can create a specially crafted PDF file that, when viewed by the target user, will trigger an overflow and execute arbitrary code with the privileges of the target user. A fixed version (3.00pl2) is available at: http://www.foolabs.com/xpdf/download.html A patch is available: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch KDE: http://www.kde.org/info/security/advisory-20041223-1.txt Gentoo: http://security.gentoo.org/glsa/glsa-200412-24.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ Mandrakesoft (update for koffice): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:165 Mandrakesoft (update for kdegraphics): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:163 Mandrakesoft (update for gpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:162 Mandrakesoft (update for xpdf): http://www.mandrakesoft.	GNU Xpdf Buffer Overflow in doImage() CVE-2004-1125	High	iDEFENSE Security Advisory 12.21.04 KDE Security Advisory, December 23, 2004 Mandrakesoft, MDKSA-2004: 161,162, 163,165, 166, December 29, 2004 Fedora Update Notification, FEDORA-2004-585, January 6, 2005 Gentoo Linux Security Advisory, GLSA 200501-13, January 10, 2005 Conectiva Linux Security Announcement, CLA-2005:921, January 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 Avaya Security Advisory, ASA-2005-027, January 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Fedora Legacy Update Advisory, FLSA:2353, February 10, 2005 Fedora Legacy Update Advisory, FLSA:2127,

	com/security/advisories?name=MDKSA-2004:161 Mandrakesoft (update for tetex): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:166 Debian: http://www.debian.org/security/2004/dsa-619 Fedora (update for tetex): http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-13.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: http://support.sgi.com/browse_request/linux_patches_by_os Conectiva: ftp://atualizacoes.conectiva.com.br/ SuSE: ftp://ftp.suse.com/pub/suse/ FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-026.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-354.html **SCO:** **ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.42/600** Currently we are not aware of any exploits for this vulnerability.			March 2, 2005 SUSE Security Announcement, SUSE-SA:2005:015, March 14, 2005 RedHat Security Advisory, RHSA-2005:026-15, March 16, 2005 SuSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005 RedHat Security Advisory, RHSA-2005:354-03, April 1, 2005 **SCO Security Advisory, SCOSA-2005.42, October 20, 2005**
Graphviz Graphviz 2.2.1	A vulnerability has been reported in '/dotty/dotty/dotty.lefty' due to the insecure creation of temporary files, which could let a malicious user overwrite arbitrary files. Update available at: http://www.graphviz.org/Download_source.php Debian: http://security.debian.org/pool/updates/main/g/graphviz/	Graphviz Insecure Temporary File Creation CVE-2005-2965	Medium	Debian Security Advisory, DSA 857-1, October 10, 2005 Ubuntu Security Notice, USN-208-1, October 17, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:188, October 21, 2005**

	Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/graphviz/ **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.			
Jan Kybic BMV 1.2	A buffer overflow vulnerability has been reported in the 'openpsfile()' function in 'gsinterf.c' due to an integer overflow error when allocating memory to store the file offsets of each page in a PS file, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	BMV Buffer Overflow CVE-2005-3278	High	Security Tracker Alert ID: 1015086, October 20, 2005
Jed Wing CHM lib 0.36, 0.35, 0.3-0.33, 0.2, 0.1	A buffer overflow vulnerability has been reported in the '_chm_decompress_block()' function due to a boundary error when reading input, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://morte.jedrea.com/~jedwin/projects/chmlib/chmlib-0.37.tgz Currently we are not aware of any exploits for this vulnerability.	CHM Lib Remote Buffer Overflow CVE-2005-3318	High	Security Focus, Bugtraq ID: 15211, October 26, 2005
KDE KOffice 1.4.1, 1.4, 1.3-1.3.5, 1.2.1, 1.2	A buffer overflow vulnerability has been reported when handling a malformed RTF file, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.koffice.org/download/ Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/k/koffice/ Gentoo: http://security.gentoo.org/glsa/glsa-200510-12.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/k/koffice/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/k/koffice/** Currently we are not aware of any exploits for this vulnerability.	KDE KOffice KWord RTF Remote Buffer Overflow CVE-2005-2971	High	Security Focus, Bugtraq ID: 15060, October 11, 2005 Ubuntu Security Notice, USN-202-1, October 12, 2005 Gentoo Linux Security Advisory, GLSA 200510-12, October 12, 2005 Fedora Update Notification, FEDORA-2005-984, October 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:185, October 14, 2005 **Debian Security Advisory, DSA 872-1, October 26, 2005**

Mgdiff mgdiff 1.0	A vulnerability has been reported in the 'viewpatch' script due to the insecure creation of temporary files, which could let a malicious user create/overwrite arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	mgdiff Insecure Temporary File Creation CVE-2005-3331	Medium	Secunia Advisory: SA17299, October 24, 2005
Mozilla Bugzilla 2.17.1, 2.17.3-2.17.7, 2.18 rc1-rc3, 2.19.1, 2.19.2	Several vulnerabilities have been reported: a vulnerability was reported because users can determine if a given invisible product exits when an access denied error is returned, which could let a remote malicious user obtain sensitive information; a vulnerability was reported because bugs can be entered into products that are closed for bug entry when a remote malicious user modifies the URL to specify the name of the product; and a vulnerability was reported because a user's password may be embedded as part of a report URL, which could let a remote malicious user obtain sensitive information. Update available at: http://www.bugzilla.org/download/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.	Bugzilla Information Disclosure CVE-2005-1563 CVE-2005-1564 CVE-2005-1565	Medium	Secunia Advisory, SA15338, May 12, 2005 **Conectiva Linux Announcement, CLSA-2005:1040, October 19, 2005**
Multiple Vendors DIA 0.91-0.94; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported in 'plug-ins/python/diasvg_import.py' due to the insecure use of the 'eval()' function when handling a malicious Scalable Vector Graphics (SVG) file, which could let a remote malicious user execute arbitrary python code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/d/dia/ Gentoo: http://security.gentoo.org/glsa/glsa-200510-06.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool/updates/main/d/dia/ **Mandriva:** **http://www.mandriva.com/security/advisories** A Proof of Concept exploit has been published.	DIA Remote Arbitrary Code Execution CVE-2005-2966	High	Security Focus, Bugtraq ID: 15000, October 3, 2005 Ubuntu Security Notice, USN-193-1, October 04, 2005 Gentoo Linux Security Advisory, GLSA 200510-06, October 6, 2005 SUSE Security Summary Report. SUSE-SR:2005:022, October 7, 2005 Debian Security Advisory DSA, 847-1, October 8, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:187, October 21, 2005**

Multiple Vendors OpenLDAP 2.1.25; Padl Software pam_ldap Builds 166, 85, 202, 199, 198, 194, 183-192, 181, 180, 173, 172, 122, 121, 113, 107, 105	A vulnerability has been reported in OpenLDAP, 'pam_ldap,' and 'nss_ldap' when a connection to a slave is established using TLS and the client is referred to a master, which could let a remote malicious user obtain sensitive information. Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-13.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/libn/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Conectiva: ftp://atualizacoes.conectiva.com.br/10/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-767.html **SGI:** **http://www.sgi.com/support/security/** There is no exploit code required.	Multiple Vendors TLS Plaintext Password CVE-2005-2069	Medium	Trustix Secure Linux Advisory, TSLSA-2005-0031, July 1, 2005 Gentoo Linux Security Advisory, GLSA 200507-13, July 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:121, July 19, 2005 Ubuntu Security Notice, USN-152-1, July 21, 2005 Turbolinux Security Advisory, TLSA-2005-86 & 87, August 29, 2006 SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005 Conectiva Linux Announcement, CLSA-2005:1027, October 14, 2005 RedHat Security Advisory, RHSA-2005:767-8, October 17, 2005 **SGI Security Advisory, 20051003-01-U, October 26, 2005**

Multiple Vendors
Glyph and Cog Xpdf 3.0, pl2 & pl3;
Ubuntu Linux 5.0 4 powerpc, i386, amd64;
RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0;
KDE 3.4.1, 3.4, 3.3.1, 3.3.2;
GNOME GPdf 2.8.3, 2.1
	A remote Denial of Service vulnerability has been reported when verifying malformed 'loca' table in PDF files.
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-670.html
	http://rhn.redhat.com/errata/RHSA-2005-671.html
	http://rhn.redhat.com/errata/RHSA-2005-708.html
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/x/xpdf/
	KDE:
	http://www.kde.org/info/security/advisory-20050809-1.txt
	Mandriva:
	http://www.mandriva.com/security/advisories
	SGI:
	ftp://patches.sgi.com/support/free/security/advisories/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200508-08.xml
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Debian:
	http://security.debian.org/pool/updates/main/k/kdegraphics/
	Trustix:
	http://http.trustix.org/pub/trustix/updates/
	TurboLinux:
	ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/10/
	Mandriva:
	http://www.mandriva.com/security/advisories
	SCO:
	ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.42/600
	Currently we are not aware of any exploits for this vulnerability.
		XPDF Loca Table Verification Remote Denial of Service
		CVE-2005-2097
			Low	RedHat Security Advisories, RHSA-2005:670-05 & RHSA-2005:671-03, & RHSA-2005:708-05, August 9, 2005
				Ubuntu Security Notice, USN-163-1, August 09, 2005
				KDE Security Advisory, 20050809-1, August 9, 2005
				Mandriva Linux Security Update Advisories, MDKSA-2005:134, 135, 136 & 138, August 11, 2005
				SGI Security Advisory, 20050802-01-U, August 15, 2005
				Gentoo Linux Security Advisory GLSA, 200508-08, August 16, 2005
				Fedora Update Notifications, FEDORA-2005-729, 730, 732, & 733, August 15 & 17, 2005
				Debian Security Advisory, DSA 780-1, August 22, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005
				Turbolinux Security Advisory, TLSA-2005-88, September 5, 2005
				Conectiva Linux Announcement, CLSA-2005:1010, September 13, 2005
				Mandriva Linux Security Update Advisory, MDKSA-2005:138-1, September 19, 2005
				SCO Security Advisory, SCOSA-2005.42, October 20, 2005

Multiple Vendors Linux Kernel Linux kernel 2.6-2.6.14	A Denial of Service vulnerability has been reported in 'net/ipv6/udp.c' due to an infinite loop error in the 'udp_v6_get_port()' function. Fedora: http://download.fedora.redhat.com/pub/fedora/	Linux Kernel IPV6 Denial of Service CVE-2005-2973	Low	Secunia Advisory: SA17261, October 21, 2005 Fedora Update Notifications, FEDORA-2005-1007 &

	linux/core/updates/ Currently we are not aware of any exploits for this vulnerability.		1013, October 20, 2005

Multiple Vendors
Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;
Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4 -5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.20;
Gentoo Linux;
GNOME GPdf 0.112;
KDE KDE 3.2-3.2.3, 3.3, 3.3.1, kpdf 3.2;
RedHat Fedora Core2;
Ubuntu ubuntu 4.1, ppc, ia64, ia32, Xpdf Xpdf 0.90-0.93; 1.0.1, 1.0 0a, 1.0, 2.0 3, 2.0 1, 2.0, 3.0,
SUSE Linux - all versions
	Several integer overflow vulnerabilities exist in 'pdftops/Catalog.cc' and 'pdftops/XRef.cc,' which could let a remote malicious user execute arbitrary code.
	Debian:
	http://security.debian.org/pool/updates/main/c/cupsys/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200410-20.xml
	KDE:
	ftp://ftp.kde.org/pub/kde/security_patches/post-3.3.1-kdegraphics.diff
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/c/cupsys/
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/
	Debian:
	http://security.debian.org/pool/updates/main/t/tetex-bin/
	SUSE: Update:
	ftp://ftp.SUSE.com/pub/SUSE
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200501-31.xml
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	FedoraLegacy:
	http://download.fedoralegacy.org/fedora/1/updates/
	RedHat:
	https://rhn.redhat.com/errata/RHSA-2005-132.html
	FedoraLegacy:
	http://download.fedoralegacy.org/redhat/
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-213.html
	SGI:
	ftp://patches.sgi.com/support/free/security/advisories/
	SUSE:
	ftp://ftp.suse.com/pub/suse/
		Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows
		CVE-2004-0888
		CVE-2004-0889
			High	Security Tracker Alert ID, 1011865, October 21, 2004
				Conectiva Linux Security Announcement, CLA-2004:886, November 8, 2004
				Debian Security Advisory, DSA 599-1, November 25, 2004
				SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004
				Gentoo Linux Security Advisory, GLSA 200501-31, January 23, 2005
				Fedora Update Notifications, FEDORA-2005-122, 123, 133-136, February 8 & 9, 2005
				Fedora Legacy Update Advisory, FLSA:2353, February 10, 2005
				Mandrakelinux Security Update Advisories, MDKSA-2005: 041-044, February 18, 2005
				RedHat Security Advisory, RHSA-2005:132-09, February, 18. 2005
				Fedora Legacy Update Advisory, FLSA:2127, March 2, 2005
				Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4, 2005
				RedHat Security Advisory, RHSA-2005:213-04, March 4, 2005
				SGI Security Advisory, 20050204-01-U, March 7, 2005
				SUSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005
				RedHat Security Advisory, RHSA-2005:354-03, April 1, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005

	RedHat: http://rhn.redhat.com/errata/RHSA-2005-354.html **Trustix:** **http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Gnome-DB libgda 1.2.1; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	Format string vulnerabilities have been reported in 'gda-log.c' due to format string errors in the 'gda_log_error()' and 'gda_log_message()' functions, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/libg/libgda2/ Currently we are not aware of any exploits for these vulnerabilities.	GNOME-DB LibGDA Multiple Format String CVE-2005-2958	High	Security Focus, Bugtraq ID: 15200, October 25, 2005 Debian Security Advisory, DSA-871-1 & 871-2, October 25, 2005
Multiple Vendors Linux kernel 2.4-2.4.29, 2.6 .10, 2.6-2.6.11	A vulnerability has been reported in the 'bluez_sock_create()' function when a negative integer value is submitted, which could let a malicious user execute arbitrary code with root privileges. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.30-rc3.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-283.html http://rhn.redhat.com/errata/RHSA-2005-284.html Conectiva: ftp://atualizacoes.conectiva.com.br/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **Another exploit script has been published.**	Linux Kernel Bluetooth Signed Buffer Index CVE-2005-0750	High	Security Tracker Alert, 1013567, March 27, 2005 SUSE Security Announcement, SUSE-SA:2005:021, April 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 US-CERT VU#685461 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005 SUSE Security Announcement, SUSE-SA:2005:29, June 9, 2005 **Security Focus, Bugtraq ID: 12911, October 24, 2005**
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to a memory leak in '/security/keys/request_key_auth.c;' a Denial of Service vulnerability was reported due to a memory leak in '/fs/namei.c' when the 'CONFIG_AUDITSYSCALL' option is enabled; and a vulnerability was reported because the orinoco wireless driver fails to pad data packets	Linux Kernel Denial of Service & Information Disclosure CVE-2005-3119 CVE-2005-3180 CVE-2005-3181	Medium	Secunia Advisory: SA17114, October 12, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005**

	with zeroes when increasing the length, which could let a malicious user obtain sensitive information. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.14-rc4.bz2 **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** There is no exploit code required.			**Fedora Update Notifications, FEDORA-2005-1013, October 20, 2005**
Multiple Vendors Linux Kernel 2.6-2.6.14	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in the 'sys_set_ mempolicy' function when a malicious user submits a negative first argument; a Denial of Service vulnerability was reported when threads are sharing memory mapping via 'CLONE_VM'; a Denial of Service vulnerability was reported in 'fs/exec.c' when one thread is tracing another thread that shares the same memory map; a Denial of Service vulnerability was reported in 'mm/ioremap.c' when performing a lookup of an non-existent page; a Denial of Service vulnerability was reported in the HFS and HFS+ (hfsplus) modules; and a remote Denial of Service vulnerability was reported due to a race condition in 'ebtables.c' when running on an SMP system that is operating under a heavy load. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Trustix:** **http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel Denials of Service CVE-2005-3053 CVE-2005-3106 CVE-2005-3107 CVE-2005-3108 CVE-2005-3109 CVE-2005-3110	Low	Ubuntu Security Notice, USN-199-1, October 10, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005**

Multiple Vendors
MandrakeSoft Multi Network Firewall 2.0, Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2, Corporate Server 3.0 x86_64, 3.0;
GNU wget 1.10;
Daniel Stenberg curl 7.14.1, 7.13.1, 7.13, 7.12.1- 7.12.3, 7.11- 7.11.2, 7.10.6- 7.10.8
	A buffer overflow vulnerability has been reported due to insufficient validation of user-supplied NTLM user name data, which could let a remote malicious user execute arbitrary code.
	WGet:
	http://ftp.gnu.org/pub/gnu/wget/wget-1.10.2.tar.gz
	Daniel Stenberg:
	http://curl.haxx.se/libcurl-ntlmbuf.patch
	Mandriva:
	http://www.mandriva.com/security/advisories
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/c/curl/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Trustix:
	http://http.trustix.org/pub/trustix/updates/
	Gentoo:
	http://security.gentoo.
		Multiple Vendor WGet/Curl NTLM Username Buffer Overflow
		CVE-2005-3185
			High	Security Tracker Alert ID: 1015056, October 13, 2005
				Mandriva Linux Security Update Advisories, MDKSA-2005:182 & 183, October 13, 200
				Ubuntu Security Notice, USN-205-1, October 14, 2005
				Fedora Update Notifications FEDORA-2005-995 & 996, October 17, 2005
				Fedora Update Notification, FEDORA-2005-1000, October 18, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005
				Gentoo Linux Security Advisory. GLSA 200510-19, October 22, 2005

	org/glsa/glsa-200510-19.xml Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, 2.1, IA64, ES 4, ES 3, 2.1, IA64, AS 4, AS 3, AS 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; OpenSSL Project OpenSSL 0.9.3-0.9.8, 0.9.2 b, 0.9.1 c; FreeBSD 6.0 -STABLE, -RELEASE, 5.4 -RELENG, -RELEASE, 5.3 -STABLE, -RELENG, -RELEASE, 5.3, 5.2.1 -RELEASE, -RELENG, 5.2 -RELEASE, 5.2, 5.1 -RELENG, -RELEASE/Alpha, 5.1 -RELEASE-p5, -RELEASE, 5.1, 5.0 -RELENG, 5.0, 4.11 -STABLE, -RELENG, 4.10 -RELENG, -RELEASE, 4.10	A vulnerability has been reported due to the implementation of the 'SSL_OP_MSIE_SSLV2_RSA_PADDING' option that maintains compatibility with third party software, which could let a remote malicious user bypass security. OpenSSL: http://www.openssl.org/source/openssl-0.9.7h.tar.gz FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:21/openssl.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-800.html Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200510-11.xml Slackware: ftp://ftp.slackware.com/pub/slackware/slackware Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101974-1 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/o/openssl/ OpenPKG: ftp://ftp.openpkg.org/release/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **SGI:** **http://www.sgi.com/support/security/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors OpenSSL Insecure Protocol Negotiation CVE-2005-2969	Medium	OpenSSL Security Advisory, October 11, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:21, October 11, 2005 RedHat Security Advisory, RHSA-2005:800-8, October 11, 2005 Mandriva Security Advisory, MDKSA-2005:179, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-11, October 12, 2005 Slackware Security Advisory, SSA:2005-286-01, October 13, 2005 Fedora Update Notifications, FEDORA-2005-985 & 986, October 13, 2005 Sun(sm) Alert Notification Sun Alert ID: 101974, October 14, 2005 Ubuntu Security Notice, USN-204-1, October 14, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.022, October 17, 2005 SUSE Security Announcement, SUSE-SA:2005:061, October 19, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005** **SGI Security Advisory, 20051003-01-U, October 26, 2005**
Multiple Vendors RedHat Fedora Core3; Linux kernel 2.6.10-2.6.13	A vulnerability has been reported because a world writable file is created in 'SYSFS' which could let a malicious user obtain sensitive information. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.13.4.tar.bz2	Linux Kernel World Writable SYSFS Information Disclosure CVE-2005-3179	Medium	Security Focus, Bugtraq ID: 15154, October 20, 2005 Fedora Update Notification FEDORA-2005-1007, October 20, 2005

	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ There is no exploit code required.			
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Netpbm 10.0	A buffer overflow vulnerability has been reported in the 'PNMToPNG' conversion package due to insufficient bounds checking of user-supplied input before coping to an insufficiently sized memory buffer, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-793.html** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200510-18.xml** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	NetPBM Buffer Overflow CVE-2005-2978	High	Ubuntu Security Notice, USN-210-1, October 18, 2005 **RedHat Security Advisory, RHSA-2005:793-6, October 18, 2005** **Gentoo Linux Security Advisory, GLSA 200510-18, October 20, 2005** **SUSE Security Summary Report, Announcement ID: SUSE-SR:2005:024, October 21, 2005** **Mandriva Linux Security Advisory, MDKSA-2005:199, October 26, 2005**
Multiple Vendors util-linux 2.8-2.13; Andries Brouwer util-linux 2.11 d, f, h, i, k, l, n, u, 2.10 s	A vulnerability has been reported because mounted filesystem options are improperly cleared due to a design flaw, which could let a remote malicious user obtain elevated privileges. Updates available at: http://www.kernel.org/pub/linux/utils/util-linux/testing/util-linux-2.12r-pre1.tar.gz Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/u/util-linux/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-15.xml Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/u/util-linux/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Conectiva: ftp://atualizacoes.	Util-Linux UMount Remounting Filesystem Elevated Privileges CVE-2005-2876	Medium	Security Focus, Bugtraq ID: 14816, September 12, 2005 Slackware Security Advisory, SSA:2005-255-02, September 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Ubuntu Security Notice, USN-184-1, September 19, 2005 Gentoo Linux Security Advisory, GLSA 200509-15, September 20, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:167, September 20, 2005 Debian Security Advisory, DSA 823-1, September 29, 2005 SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005 Conectiva Linux Announcement, CLSA-2005:1022, October 6, 2005 Sun(sm) Alert Notification Sun Alert ID: 101960, October 10, 2005 **SGI Security Advisor,**

	conectiva.com.br/ 10/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101960-1 **SGI: http://www.sgi.com/support/security/** There is no exploit code required.		**20051003-01-U, October 26, 2005**

Multiple Vendors XFree86 X11R6 4.3 .0, 4.1 .0; X.org X11R6 6.8.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Advanced Workstation for the Itanium Processor 2.1, IA64; Gentoo Linux	A buffer overflow vulnerability has been reported in the pixmap processing code, which could let a malicious user execute arbitrary code and possibly obtain superuser privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200509-07.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-329.html http://rhn.redhat.com/errata/RHSA-2005-396.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ Mandriva: http://www.mandriva.com/security/advisories?name=MDKSA-2005:164 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/x/xfree86/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101926-1&searchclause SUSE: ftp://ftp.suse.com/pub/suse/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101953-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-218.pdf **Sun 101926: Updated Contributing Factors, Relief/Workaround, and Resolution sections.** Currently we are not aware of any exploits for this vulnerability.	XFree86 Pixmap Allocation Buffer Overflow CVE-2005-2495	High	Gentoo Linux Security Advisory, GLSA 200509-07, September 12, 2005 RedHat Security Advisory, RHSA-2005:329-12 & RHSA-2005:396-9, September 12 & 13, 2005 Ubuntu Security Notice, USN-182-1, September 12, 2005 Mandriva Security Advisory, MDKSA-2005:164, September 13, 2005 US-CERT VU#102441 Fedora Update Notifications, FEDORA-2005-893 & 894, September 16, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Debian Security Advisory DSA 816-1, September 19, 2005 Sun(sm) Alert Notification Sun Alert ID: 101926, September 19, 2005 SUSE Security Announcement, SUSE-SA:2005:056, September 26, 2005 Slackware Security Advisory, SSA:2005-269-02, September 26, 2005 Sun(sm) Alert Notification Sun Alert ID: 101953, October 3, 2005 SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 Avaya Security Advisory, ASA-2005-218, October 19, 2005 **Sun(sm) Alert Notification Sun Alert ID: 101926, Updated October 24, 2005**
Multiple Vendors xine xine-lib 1.1.0, 1.0-1.0.2, 0.9.13; Ubuntu Linux 5.0 4 powerpc, i386, amd64, ppc, ia64, ia32; Gentoo Linux	A format string vulnerability has been reported in 'input_cdda.c' when writing CD metadata retrieved from a CDDB server to a cache file, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200510-08.xml Ubuntu:	Multiple Vendors CDDB Client Format String CVE-2005-2967	High	Gentoo Linux Security Advisory, GLSA 200510-08, October 8, 2005 Ubuntu Security Notice, USN-196-1, October 10, 2005 Slackware Security Advisory, SSA:2005-283-01, October

	http://security.ubuntu.com/ubuntu/pool/main/x/xine-lib/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/x/xine-lib/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** An exploit script has been published.			11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:180, October 11, 2005 Debian Security Advisory, DSA 863-1, October 12, 2005 Conectiva Linux Announcement, CLSA-2005:1026, October 11, 2005 **SUSE Security Summary Report, SUSE-SR:2005:024, October 21, 2005**
Net-SNMP Net-SNMP 5.2.1, 5.2, 5.1-5.1.2, 5.0.3 -5.0.9, 5.0.1	A remote Denial of Service vulnerability has been reported when handling stream-based protocols. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=12694&package_id =11571&release_id=338899 Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-720.html Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/net-snmp/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-395.html Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-225.pdf **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Debian:** **http://security.debian.**	Net-SNMP Protocol Denial of Service CVE-2005-2177	Low	Secunia Advisory: SA15930, July 6, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Fedora Update Notifications, FEDORA-2005-561 & 562, July 13, 2005 RedHat Security Advisory, RHSA-2005:720-04, August 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:137, August 11, 2005 Ubuntu Security Notice, USN-190-1, September 29, 2005 RedHat Security Advisory, RHSA-2005:395-18, October 5, 2005 Conectiva Linux Announcement, CLSA-2005:1032, October 13, 2005 Avaya Security Advisory, ASA-2005-225, October 18, 200 **SUSE Security Summary Report, Announcement ID: SUSE-SR:2005:024, October 21, 2005** **Debian Security Advisory, DSA 873-1, October 26, 2005**

	org/pool/updates/main/n/net-snmp/ Currently we are not aware of any exploits for this vulnerability.			
Padl Software pam_ldap Build 179, Build 169	A vulnerability has been reported when handling a new password policy control, which could let a remote malicious user bypass authentication policies. Upgrades available at: ftp://ftp.padl.com/pub/pam_ldap.tgz Gentoo: http://security.gentoo.org/glsa/glsa-200508-22.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-767.html **Mandriva:** **http://www.mandriva.com/security/advisories** **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** There is no exploit code required.	PADL Software PAM_LDAP Authentication Bypass CVE-2005-2641	Medium	Bugtraq ID: 14649, August 24, 2005 US-CERT VU#778916 Gentoo Linux Security Advisory, GLSA 200508-22, August 31, 2005 Conectiva Linux Announcement, CLSA-2005:1027, October 14, 2005 RedHat Security Advisory, RHSA-2005:767-8, October 17, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:190, October 21, 2005** **SGI Security Advisory, 20051003-01-U, October 26, 2005**
PCRE PCRE 6.1, 6.0, 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available at: http://www.pcre.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/pcre3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-17.xml Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/	PCRE Regular Expression Heap Overflow CVE-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 Ubuntu Security Notices, USN-173-1 & 173-2, August 24, 2005 Fedora Update Notifications, FEDORA-2005-802 & 803, August 24, 2005 Gentoo Linux Security Advisory, GLSA 200508-17, August 25, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:151-155, August 25, 26, & 29, 2005 SUSE Security Announcements, SUSE-SA:2005:048 & 049, August 30, 2005 Slackware Security Advisories, SSA:2005-242-01 & 242-02, August 31, 2005 Ubuntu Security Notices, USN-173-3, 173-4 August 30 & 31, 2005 Debian Security Advisory, DSA 800-1, September 2, 2005 SUSE Security Announcement,

	Debian: http://security.debian.org/pool/updates/main/p/pcre3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.1/testing/packages/php-5.0.5/php-5.0.5-i486-1.tgz Gentoo: http://security.gentoo.org/glsa/glsa-200509-08.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-12.xml Debian: http://security.debian.org/pool/updates/main/p/python2.2/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-19.xml Debian: http://security.debian.org/pool/updates/main/p/python2.3/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-216.pdf **Trustix:** **http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for this vulnerability.			SUSE-SA:2005:051, September 5, 2005 Slackware Security Advisory, SSA:2005-251-04, September 9, 2005 Gentoo Linux Security Advisory, GLSA 200509-08, September 12, 2005 Conectiva Linux Announcement, CLSA-2005:1009, September 13, 2005 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 Debian Security Advisory, DSA 817-1 & DSA 819-1, September 22 & 23, 2005 Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005 Debian Security Advisory, DSA 821-1, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005 Turbolinux Security Advisory, TLSA-2005-92, October 3, 2005 Avaya Security Advisory, ASA-2005-216, October 18, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005**
PHP PHP 5.0 .0-5.0.5, 4.4 .0, 4.3.1 -4.3.11, 4.2-4.2.3, 4.1.0-4.1.2, 4.0 0-4.0.7	A Denial of Service vulnerability has been reported in the 'sapi_apache2.c' file. PHP 5.1.0 final and 4.4.1 final are not affected by this issue. Please contact the vendor to obtain fixes. There is no exploit code required.	PHP Apache 2 Denial of Service CVE-2005-3319	Low	Security Focus, Bugtraq ID: 15177, October 24, 2005
phpMyAdmin phpMyAdmin 2.6.4 -pl1	A vulnerability has been reported in 'libraries/grab_globals.lib.php' due to insufficient verification of the 'subform' array parameter before including files, which could let a malicious user include arbitrary files. Gentoo:	PHPMyAdmin File Include CVE-2005-3299	Medium	Secunia Advisory: SA17137, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-16, October 17, 2005

	http://security.gentoo.org/glsa/glsa-200510-16.xml **Upgrades available at:** **http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.6.4-pl3.tar .gz** There is no exploit code required; however, a Proof of Concept exploit script has been published.			**Security Focus Bugtraq ID: 15053, October 22, 2005**
phpMyAdmin phpMyAdmin 2.x	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient verification of certain configuration parameters, which could let a remote malicious user include arbitrary files; and a Cross-Site Scripting vulnerability was reported in 'left.php,' 'queryframe.php,' and 'server_databases.php' due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.6.4-pl3.tar .gz Gentoo: http://security.gentoo.org/glsa/glsa-200510-21.xml There is no exploit code required; however, a Proof of Concept exploit has been published.	phpMyAdmin Local File Inclusion & Cross-Site Scripting CVE-2005-3301	Medium	Secunia Advisory: SA17289, October 24, 2005 Gentoo Linux Security Advisory, GLSA 200510-21, October 25, 2005
SCO Open Server 5.0.7	A buffer overflow vulnerability has been reported in 'Backupsh' when processing excessive data, which could let a malicious user execute arbitrary code. Update available at: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.40 Currently we are not aware of any exploits for this vulnerability.	SCO OpenServer 'Backupsh' Buffer Overflow CVE-2005-2926	High	SCO Security Advisory, SCOSA-2005.40, October 20, 2005
SCO Unixware 7.1.4, 7.1.3	A buffer overflow vulnerability has been reported in the PPP binary, which could let a malicious user obtain root privileges. Updates available at: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.41 Currently we are not aware of any exploits for this vulnerability.	SCO UnixWare PPP Prompt Buffer Overflow CVE-2005-2927	High	SCO Security Advisory, SCOSA-2005.41, October 20, 2005
SiteTurn Domain Manager Pro	A Cross-Site Scripting vulnerability has been reported in the 'panel' script due to insufficient sanitization of the 'err 'parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	SiteTurn Domain Manager Pro Admin Panel Cross-Site Scripting CVE-2005-3320	Medium	KAPDA::#8 Advisory, October 25, 2005
Squid Squid 2.x	A remote Denial of Service vulnerability has been reported when handling certain FTP server responses. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE11-rfc1738_do_escape.patch	Squid FTP Server Response Handling Remote Denial of Service CVE-2005-3258	Low	Secunia Advisory: SA17271, October 20, 2005 Fedora Update Notifications, FEDORA-2005-1009 & 1010, October 20, 2005 Mandriva Linux Security Advisory,

	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories There is no exploit code required.			MDKSA-2005:195, October 26, 2005
SuSE SuSE Linux Professional 9.0, x86_64, Linux Personal 9.0, x86_64	A remote Denial of Service vulnerability has been reported in the squid proxy when handling specially crafted HTTPs data. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	SUSE Linux Squid Proxy SSL Handling Remote Denial of Service CVE-2005-3322	Low	SUSE Security Summary Report, Announcement ID: SUSE-SR:2005:024, October 21, 2005
SuSE UnitedLinux 1.0, Linux Professional 10.0 OSS, 10.0, 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, 9.0, x86_64, Linux Personal 10.0 OSS, 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, 9.0, x86_64, Linux Enterprise Server 9, 8, Linux Desktop 1.0	A vulnerability has been reported in the 'permissions' package due to file permissions improper handling by the 'chkstat' utility, which could let a malicious user obtain sensitive information. SUSE: ftp://ftp.SUSE.com/pub/SUSE There is no exploit code required.	SUSE Linux Permissions Package CHKSTAT Information Disclosure CVE-2005-3321	Medium	SUSE Security Announcement, SUSE-SA:2005:062, October 24, 2005
Symantec Norton Utilities for Macintosh 8.0, Norton System Works for Macintosh 3.0, Norton Personal Firewall for Macintosh 3.1, 3.0, Norton Internet Security for Macintosh 3.0, Norton Antivirus for Macintosh 10.0.1, 10.0 .0, 9.0.0-9.0.3, LiveUpdate for Macintosh 3.5, 3.0-3.0.3	Several vulnerabilities have been reported: a vulnerability was reported in the 'DiskMountNotify' component of Symantec Norton AntiVirus for Macintosh due to failure to use the execution path environment, which could let a malicious user execute arbitrary commands with System Administrative privileges; and a vulnerability was reported in the liveupdate component because the '/Library/Application Support/Norton Solutions Support/LiveUpdate/jlucaller' command-line application is used to interface with the Java interpreter, which could let a malicious user execute arbitrary Java code with System Administrative privileges. Symantec has released a patch to address this issue. This patch can be automatically installed on vulnerable computers by running LiveUpdate. There is no exploit code required.	Symantec AntiVirus/ LiveUpdate for Macintosh System Admin Privileges CVE-2005-2759	High	Security Tracker Alert IDs: 1015083 & 1015084, October 20, 2005
Todd Miller Sudo 1.x	A vulnerability has been reported in the environment cleaning due to insufficient sanitization, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/s/sudo/ There is no exploit code required.	Todd Miller Sudo Local Elevated Privileges CVE-2005-2959	Medium	Debian Security Advisory, DSA 870-1, October 25, 2005
University of Washington UW-imapd imap-2004c1	A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version imap-2004g: ftp://ftp.cac.washington.edu/imap/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/u/uw-imap/ Gentoo: http://security.gentoo.org/glsa/glsa-	UW-imapd Denial of Service and Arbitrary Code Execution CVE-2005-2933	High	Secunia, Advisory: SA17062, October 5, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005 Debian Security Advisory, DSA 861-1, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-10, October 11, 2005 US-CERT VU#933601 SUSE Security Summary Report,

	200510-10.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE **Mandriva:** **http://www.mandriva.com/ security/advisories** Currently we are not aware of any exploits for this vulnerability.			SUSE-SR:2005:023, October 14, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:189 & 194 , October 21 & 26, 2005**
Webmin Webmin 1.220, 1.210, 1.200; Usermin 1.150, 1.140, 1.130	A vulnerability has been reported in 'miniserv.pl' due to an input validation error in the authentication process, which could let a remote malicious user bypass certain security restrictions. Webmin: http://prdownloads.sourceforge.net/webadmin/webmin-1.230.tar.gz Usermin: http://prdownloads.sourceforge.net/webadmin/usermin-1.160.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200509-17.xml Mandriva: http://www.mandriva.com/security/advisories **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Webmin / Usermin Remote PAM Authentication Bypass CVE-2005-3042	Medium	SNS Advisory No.83, September 20, 2005 Gentoo Linux Security Advisory, GLSA 200509-17, September 24, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:176, October 7, 2005 **SUSE Security Summary Report, Announcement ID: SUSE-SR:2005:024, October 21, 2005**
xloadimage xloadimage 4.1	A buffer overflow vulnerability has been reported when handling the title of a NIFF image when performing zoom, reduce, or rotate functions, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/x/xloadimage/ http://security.debian.org/pool/updates/main/x/xli/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-802.html **Mandriva:** **http://www.mandriva.com/security/advisories** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **SGI:** **http://www.sgi.com/support/security/** Currently we are not aware of any exploits for this vulnerability.	Xloadimage NIFF Image Buffer Overflow CVE-2005-3178	High	Debian Security Advisories, DSA 858-1 & 859-1, October 10, 2005 RedHat Security Advisory, RHSA-2005:802-4, October 18, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:191, October 21, 2005** **SUSE Security Summary Report, SUSE-SR:2005:024, October 21, 2005** **SGI Security Advisory, 20051003-01-U, October 26, 2005**
Yukihiro Matsumoto Ruby 1.6 - 1.6.8, 1.8 - 1.8.2	A vulnerability has been reported in 'eval.c' due to a flaw in the logic that implements the SAFE level checks, which could let a remote malicious user bypass access restrictions to execute	Ruby Safe Level Restrictions Bypass	Medium	Security Tracker Alert ID: 1014948, September 21, 2005

	scripting code. Patches available at: ftp://ftp.ruby-lang.org/pub/ruby/1.6/1.6.8-patch1.gz Updates available at: http://www.ruby-lang.org/patches/ruby-1.8.2-xmlrpc-ipimethods-fix.diff Gentoo: http://security.gentoo.org/glsa/glsa-200510-05.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/r/ruby1.8/ Debian: http://security.debian.org/pool/updates/main/r/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-799.html Debian: http://security.debian.org/pool/updates/main/r/ruby1.8/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Mandriva: http://www.mandriva.com/security/advisories** **RedHat: http://rhn.redhat.com/errata/RHSA-2005-799.html** **SGI: http://www.sgi.com/support/security/** There is no exploit code required.	CVE-2005-2337		US-CERT VU#160012 Gentoo Linux Security Advisory, GLSA 200510-05, October 6, 2005 Ubuntu Security Notice, USN-195-1, October 10, 2005 Debian Security Advisories, DSA 860-1 & DSA 862-1, October 11, 2005 RedHat Security Advisory, RHSA-2005:799-3, October 11, 2005 Debian Security Advisory, DSA 864-1, October 13, 2005 Conectiva Linux Announcement, CLSA-2005:1030, October 13, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:191, October 21, 2005** **RedHat Security Advisory, RHSA-2005:799-6, Updated October 25, 2005** **SGI Security Advisory, 20051003-01-U, October 26, 2005**
Zope Zope 2.6-2.8.1	A vulnerability has been reported in 'docutils' due to an unspecified error and affects all instances which exposes 'RestructuredText' functionality via the web. The impact was not specified. Hotfix available at: http://www.zope.org/Products/Zope/Hotfix_2005-10-09/security_alert/Hot fix_2005-10-09.tar.gz **Gentoo: http://security.gentoo.org/glsa/glsa-200510-20.xml** Currently we are not aware of any exploits for this vulnerability.	Zope 'Restructured Text' Unspecified Security Vulnerability CVE-2005-3323	Not Specified	Zope Security Alert, October 12, 2005 **Gentoo Linux Security Advisory, GLSA 200510-20, October 25, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Abi Source Community AbiWord 2.2.0-2.2.10, 2.2.12, 2.0.1-2.0.9	Multiple stack-based buffer overflow vulnerabilities have been reported due to insufficient bounds checking of user-supplied data prior to copying it to an insufficiently sized memory buffer while importing RTF files, which could let a remote malicious user execute arbitrary code. The vendor has addressed this issue in AbiWord version 2.2.11. Users are advised to contact the vendor to obtain the appropriate update. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/abiword/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200510-17.xml** Currently we are not aware of any exploits for these vulnerabilities.	AbiWord Stack-Based Buffer Overflows CVE-2005-2972	High	Ubuntu Security Notice, USN-203-1, October 13, 2005 Fedora Update Notification, FEDORA-2005-989, October 13, 2005 Conectiva Linux Announcement, CLSA-2005:1035, October 14, 2005 **Gentoo Linux Security Advisory, GLSA 200510-17, October 20, 2005**
AL-Caricatier AL-Caricatier 2.5, 1.0	A vulnerability has been reported in 'ss.php' due to an insecure process, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	AL-Caricatier SS.PHP Authentication Bypass	Medium	Secunia Advisory: SA17292, October 24, 2005

Apache	A vulnerability has been reported in Apache which can be exploited by remote malicious users to smuggle http requests. Conectiva: http://distro.conectiva.com.br/ atualizacoes/index.php?id=a&anuncio=000982 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ SuSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/a/apache/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ IBM has released fixes for Hardware Management Console addressing this issue. Users should contact IBM for further information. **Trustix:** **http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for this vulnerability.	Apache HTTP Request Smuggling Vulnerability CVE-2005-1268 CVE-2005-2088	Medium	Secunia, Advisory: SA14530, July 26, 2005 Conectiva, CLSA-2005:982, July 25, 2005 Fedora Update Notification FEDORA-2005-638 & 639, August 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:129, August 3, 2005 Ubuntu Security Notice, USN-160-1, August 04, 2005 Turbolinux Security Advisory, TLSA-2005-81, August 9, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 SUSE Security Announcement, SUSE-SA:2005:046, August 16, 2005 Debian Security Advisory DSA 803-1, September 8, 2005 Ubuntu Security Notice, USN-160-2, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Security Focus, Bugtraq ID: 14106, September 21, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005**
AppIndex MWChat 6.8	An SQL injection vulnerability has been reported in 'chat.php' due to insufficient sanitization of the 'username' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	MWChat SQL Injection CVE-2005-3324	Medium	Security Tracker Alert ID: 1015094, October 24, 2005
ar-blog ar-blog 5.2, 2.0	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input when adding a comment, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported due to an insecure authentication process, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	ar-blog Cross-SIte Scripting & Authentication Bypass	Medium	Security Tracker Alert ID: 1015100, October 25, 2005
BASE Basic Analysis and Security Engine BASE Basic Analysis and Security Engine 1.2	An SQL injection vulnerability has been reported in 'base_qry_main.php' due to insufficient sanitization of the 'sig[1] parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept	Basic Analysis and Security Engine SQL Injection CVE-2005-3325	Medium	Secunia Advisory: SA17314, October 25, 2005

	exploit has been published.			
Belchior Foundry vCard 2.9	A file include vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Belchior Foundry VCard Remote File Include CVE-2005-3332	High	Security Focus, Bugtraq ID: 15207, October 26, 2005
Chipmunk PHP Scripts Chipmunk Topsites, Forum, Directory	Cross-Site Scripting vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'newtopic.php,' 'quote.php,' 'index.php,' and 'reply.php' due to insufficient sanitization of the 'forum_ID' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability was reported in 'recommend.php' due to insufficient sanitization of the 'ID' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Chipmunk Multiple Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 15149, October 20, 2005
Digital Dominion PHP-Fusion 6.0.204	A vulnerability has been reported in the 'submit.php' script due to insufficient sanitization of the 'news_body' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	PHP-Fusion Script Insertion	Medium	Secunia Advisory: SA17312, October 25, 2005
eBASE web eBASEweb 3.0	An SQL injection vulnerability has been reported due to insufficient sanitization of input passed to certain parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrade available at: http://www.ebase.co.jp/company/security/ There is no exploit code required.	eBASEweb SQL Injection CVE-2005-3333	Medium	Security Tracker Alert ID: 1015089, October 21, 2005
FlatNuke FlatNuke 2.5.1-2.5.6	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in 'index.php' due to insufficient verification of the 'user' and 'quale' parameters before used to show file context, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 'user' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://flatnuke.sourceforge.net/nightly/flatnuke-2.5.7-20051024.tar.gz There is no exploit code required; however, Proof of Concept exploits have been published.	FlatNuke Cross-Site Scripting & Directory Traversal CVE-2005-3306 CVE-2005-3307	Medium	Secunia Advisory: SA17291, October 24, 2005
Flyspray Flyspray 0.9.8 development, 0.9.8, 0.9.7	Cross-Site Scripting vulnerabilities have been reported in 'index.php' due to insufficient sanitization of input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit URLs have been published.	Flyspray Multiple Cross-Site Scripting CVE-2005-3334	Medium	Flyspray Security Advisory, FS#703, October 24, 2005
Francisco Burzi PHP-Nuke 7.8	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHPNuke Multiple Modules SQL Injection CVE-2005-3304	Medium	Security Focus, Bugtraq ID: 15178, October 24, 2005

ipbPro Arcade ipbProArcade 2.5.2	An SQL injection vulnerability has been reported in the 'gameid' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	IPBProArcade Remote SQL Injection	Medium	Security Focus, Bugtraq ID: 15205, October 26, 2005
Mantis Mantis 1.0.0RC2, 0.19.2	Several vulnerabilities have been reported: a vulnerability was reported in 'bug_ sponsorship_list_view_inc.php' due to insufficient verification before used to include files, which could let a remote malicious user execute arbitrary files; an SQL injection vulnerability was reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; several Cross-Site Scripting vulnerabilities were reported in JavaScript and 'mantis/view_all_set.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; an unspecified vulnerability was reported when using reminders, which could lead to the disclosure of sensitive information; and a vulnerability was reported because caches the User ID longer than necessary. Upgrades available at: http://prdownloads.sourceforge.net/mantisbt/mantis-0.19.3.tar.gz There is no exploit code required; however, Proof of Concept exploits have been published.	Mantis Multiple Vulnerabilities CVE-2005-3335 CVE-2005-3336 CVE-2005-3337 CVE-2005-3338 CVE-2005-3339	High	Secunia Advisory: SA16818, October 26, 2005
Mozilla Firefox 1.0.6; Mozilla Browser 1.7.11, 1.7-1.7.9; Thunderbird 1.0-1.0.6	A vulnerability has been reported which could let a remote malicious user execute arbitrary commands via shell metacharacters in a URL. Upgrades available at: http://www.mozilla.org/products/firefox/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-785.html http://rhn.redhat.com/errata/RHSA-2005-789.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.479350 SGI: ftp://patches.sgi.com/support/free/security/advisories/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux:	Mozilla Browser/Firefox Arbitrary Command Execution CVE-2005-2968	High	Security Focus Bugtraq ID: 14888, September 21, 2005 Security Focus Bugtraq ID: 14888, September 22, 2005 RedHat Security Advisories, RHSA-2005:785-9 & 789-11, September 22, 2005 Ubuntu Security Notices, USN-USN-186-1 & 186-2, September 23 & 25, 2005 US-CERT VU#914681 Mandriva Linux Security Update Advisory, MDKSA-2005:169, September 26, 2005 Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 SGI Security Advisory, 20050903-02-U, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005 Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005 Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005 Slackware Security Advisory,

	ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla/** **http://security.debian.org/pool/updates/main/m/mozilla-thunderbird/** There is no exploit code required; however, a Proof of Concept exploit has been published.			SSA:2005-278-01, October 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005 Ubuntu Security Notice, USN-200-1, October 11, 2005 **Debian Security Advisories, DSA 866-1 & 868-1, October 20, 2005**

Mozilla.org
Netscape 8.0.3.3, 7.2;
Mozilla Firefox 1.5 Beta1, 1.0.6;
Mozilla Browser 1.7.11; Mozilla Thunderbird 1.0.6
	A buffer overflow vulnerability has been reported due to an error when handling IDN URLs that contain the 0xAD character in the domain name, which could let a remote malicious user execute arbitrary code.
	Patches available at:
	http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-769.html
	http://rhn.redhat.com/errata/RHSA-2005-768.html
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200509-11.xml
	Slackware:
	ftp://ftp.slackware.com/pub/slackware/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200509-11.xml
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/10/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Debian:
	http://security.debian.org/pool/updates/
		Mozilla/Netscape/Firefox Browsers Domain Name Buffer Overflow
		CVE-2005-2871
			High	Security Focus, Bugtraq ID: 14784, September 10, 2005
				RedHat Security Advisories, 769-8 & RHSA-2005:768-6, September 9, 2005
				Fedora Update Notifications, FEDORA-2005-871-184, September 10, 2005
				Ubuntu Security Notice, USN-181-1, September 12, 2005
				US-CERT VU#573857
				Gentoo Linux Security Advisory GLSA 200509-11, September 18, 2005
				Security Focus, Bugtraq ID: 14784, September 22, 2005
				Slackware Security Advisory, SSA:2005-269-01, September 26, 2005
				Gentoo Linux Security Advisory [UPDATE], GLSA 200509-11:02, September 29, 2005
				Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005
				Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005
				Debian Security Advisory, DSA 837-1, October 2, 2005
				Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005

	main/m/mozilla-firefox/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ HP: http://software.hp.com/ Mandriva: http://www.mandriva.com/security/advisories HPSBUX01231 Rev1: Preliminary Mozilla 1.7.12 available. Netscape: http://browser.netscape.com/ns8/download/default.jsp **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla/** **http://security.debian.org/pool/updates/main/m/mozilla-thunderbird/** A Proof of Concept exploit script has been published.			HP Security Bulletin, HPSBUX01231, October 3, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005 HP Security Bulletin, HPSBUX01231 Rev 1, October 12, 2005 **Debian Security Advisories, DSA 866-1 & 868-1, October 20, 2005**
Multiple Vendors Mozilla Firefox 1.0-1.0.6; Mozilla Browser 1.7-1.7.11; Netscape Browser 8.0.3.3	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when processing malformed XBM images, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when unicode sequences contain 'zero-width non-joiner' characters, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability was reported due to a flaw when making XMLHttp requests, which could let a remote malicious user spoof XMLHttpRequest headers; a vulnerability was reported because a remote malicious user can create specially crafted HTML that spoofs XML objects to create an XBL binding to execute arbitrary JavaScript with elevated (chrome) permissions; an integer overflow vulnerability was reported in the JavaScript engine, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported because a remote malicious user can load privileged 'chrome' pages from an unprivileged 'about:' page, which could lead to unauthorized access; and a window spoofing vulnerability was reported when a blank 'chrom' canvas is obtained by opening a window from a reference to a closed window, which could let a remote malicious user conduct phishing type attacks. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-789.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/	Mozilla Browser / Firefox Multiple Vulnerabilities CVE-2005-2701 CVE-2005-2702 CVE-2005-2703 CVE-2005-2704 CVE-2005-2705 CVE-2005-2706 CVE-2005-2707	High	Mozilla Foundation Security Advisory, 2005-58, September 22, 2005 RedHat Security Advisory, RHSA-2005:789-11, September 22, 2005 Ubuntu Security Notices, USN-186-1 & 186-2, September 23 & 25, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:169 & 170, September 26, 2005 Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 SGI Security Advisory, 20050903-02-U, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005 Gentoo Linux Security Advisory [UPDATE], September 29, 2005 SUSE Security Announcement, SUSE-SA:2005:058, September 30, 2005 Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005 Debian Security Advisory, DSA 838-1, October 2, 2005

	security/viewer.php?l=slackware-security&y=2005&m=slackware-security.479350 SGI: ftp://patches.sgi.com/support/free/security/advisories/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ Netscape: http://browser.netscape.com/ns8/download/default.jsp **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla/** **http://security.debian.org/pool/updates/main/m/mozilla-thunderbird/** Currently we are not aware of any exploits for these vulnerabilities.			Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005 Ubuntu Security Notice, USN-200-1, October 11, 2005 Security Focus, Bugtraq ID: 14916, October 19, 2005 **Debian Security Advisories, DSA 866-1 & 868-1, October 20, 2005**
Multiple Vendors Snort Project Snort 2.4.0-2.4.2; Nortel Networks Threat Protection System Intrusion Sensor 4.1, Nortel Networks Threat Protection System Defense Center 4.1	A buffer overflow vulnerability has been reported in the Back Orifice processor due to a failure to securely copy network-derived data into sensitive process buffers, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.snort.org/dl/current/snort-2.4.3.tar.gz Nortel: http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=SWDETAIL&SoftwareOID=362101 **Exploit scripts have been published.**	Snort Back Orifice Preprocessor Remote Buffer Overflow CVE-2005-3252	High	Internet Security Systems Protection Advisory, October 18, 2005 Technical Cyber Security Alert TA05-291A, October 18, 2005 US-CERT VU#175500 **Security Focus, Bugtraq ID: 15131, October 25, 2005**

Multiple Vendors Gentoo Linux; Apache Software Foundation Apache 2.1-2.1.5, 2.0.35-2.0.54, 2.0.32, 2.0.28, Beta, 2.0 a9, 2.0	A remote Denial of Service vulnerability has been reported in the HTTP 'Range' header due to an error in the byte-range filter. Patches available at: http://issues.apache.org/bugzilla/attachment.cgi?id=16102 Gentoo: http://security.gentoo.org/glsa/glsa-200508-15.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Debian: http://security.debian.org/pool/updates/main/a/apache2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-204.pdf Conectiva: ftp://atualizacoes.conectiva.com.br/10/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Trustix:** **http://http.trustix.org/pub/trustix/updates/** There is no exploit code required.	Apache Remote Denial of Service CVE-2005-2728	Low	Secunia Advisory: SA16559, August 25, 2005 Security Advisory, GLSA 200508-15, August 25, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 Fedora Update Notifications, FEDORA-2005-848 & 849, September 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Debian Security Advisory, DSA 805-1, September 8, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005 Avaya Security Advisory, ASA-2005-204, September 23, 2005 Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005 Turbolinux Security Advisory, TLSA-2005-94, October 3, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005**
Multiple Vendors RedHat Fedora Core4, Core3; Ethereal Group Ethereal 0.10 -0.10.12, 0.9-0.9.16, 0.8.19, 0.8.18	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the ISAKMP, FC-FCS, RSVP, and ISIS LSP dissectors; a remote Denial of Service vulnerability was reported in the IrDA dissector; a buffer overflow vulnerability was reported in the SLIMP3, AgentX, and SRVLOC dissectors, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in the BER dissector; a remote Denial of Service vulnerability was reported in the SigComp UDVM dissector; a remote Denial of service vulnerability was reported due to a null pointer dereference in the SCSI, sFlow, and RTnet dissectors; a vulnerability was reported because a remote malicious user can trigger a divide by zero error in the X11 dissector; a vulnerability was reported because a remote malicious user can cause an invalid pointer to be freed in the WSP dissector; a remote Denial of Service vulnerability was reported if the 'Dissect unknown RPC program numbers' option is enabled (not the default setting); and a remote Denial of Service	Ethereal Multiple Protocol Dissector Vulnerabilities CVE-2005-3184 CVE-2005-3241 CVE-2005-3242 CVE-2005-3243 CVE-2005-3244 CVE-2005-3245 CVE-2005-3246 CVE-2005-3247 CVE-2005-3248 CVE-2005-3249	High	Ethereal Security Advisory, enpa-sa-00021, October 19, 2005 Fedora Update Notifications, FEDORA-2005-1008 & 1011, October 20, 2005 RedHat Security Advisory, RHSA-2005:809-6, October 25, 2005 Mandriva Linux Security Advisory, MDKSA-2005:193, October 25, 2005

	vulnerability was reported if SMB transaction payload reassembly is enabled (not the default setting). Upgrades available at: http://prdownloads.sourceforge.net/ethereal/ethereal-0.10.13.tar.gz?download Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-809.html Mandriva: http://www.mandriva.com/security/advisories An exploit script has been published.			

Multiple Vendors
Ukranian National Antivirus UNA;
Trend Micro PC-cillin 2005, OfficeScan Corporate Edition 7.0;
Sophos Anti-Virus 3.91;
Panda Titanium Norman Virus Control 5.81;
McAfee Internet Security Suite 7.1.5;
Kaspersky Labs Anti-Virus 5.0.372;
Ikarus Ikarus 2.32;
F-Prot Antivirus 3.16 c;
eTrust CA 7.0.14;
Dr.Web 4.32 b; AVG Anti-Virus 7.0.323;
ArcaBit ArcaVir 2005.0
	A vulnerability has been reported in the scanning engine routine that determines the file type if the MAGIC BYTE of the EXE files is at the beginning, which could lead to a false sense of security and arbitrary code execution.
	No workaround or patch available at time of publishing.
	A Proof of Concept exploit has been published.
		Multiple Vendors Anti-Virus Magic Byte Detection Evasion	High	Security Focus, Bugtraq ID: 15189, October 25, 2005

Multiple Vendors University of Kansas Lynx 2.8.6 dev.1-dev.13, 2.8.5 dev.8, 2.8.5 dev.2-dev.5, 2.8.5, 2.8.4 rel.1, 2.8.4, 2.8.3 rel.1, 2.8.3 pre.5, 2.8.3 dev2x, 2.8.3 dev.22, 2.8.3, 2.8.2 rel.1, 2.8.1, 2.8, 2.7; RedHat Enterprise Linux WS 4, WS 3, 2.1, ES 4, ES 3, ES 2.1, AS 4, AS 3, AS 2.1, RedHat Desktop 4.0, 3.0, RedHat Advanced Workstation for the Itanium Processor 2.1 IA64	A buffer overflow vulnerability has been reported in the 'HTrjis()' function when handling NNTP article headers, which could let a remote malicious user execute arbitrary code. University of Kansas Lynx: http://lynx.isc.org/current/lynx2.8.6dev.14.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200510-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lynx/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-803.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Trustix:**	Lynx 'HTrjis()' NNTP Remote Buffer Overflow CVE-2005-3120	High	Gentoo Linux Security Advisory, GLSA 200510-15, October 17, 2005 Ubuntu Security Notice, USN-206-1, October 17, 2005 RedHat Security Advisory, RHSA-2005:803-4, October 17, 2005 Fedora Update Notifications, FEDORA-2005-993 & 994, October 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:186, October 18, 2005 Conectiva Linux Announcement, CLSA-2005:1037, October 19, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005** **SGI Security Advisory, 20051003-01-U, October 26, 2005**

	http://http.trustix.org/ pub/trustix/updates/ **SGI:** **http://www.sgi.com/ support/security/** **Mandriva:** **http://www.mandriva.com/ security/advisories** **Debian:** **http://security.debian. org/pool/updates/ main/l/lynx/** **http://security.debian. org/pool/updates/ main/l/lynx-ssl/** A Proof of Concept Denial of Service exploit script has been published.			**Mandriva Linux Security Advisory, MDKSA-2005:186-1, October 26, 2005** **Debian Security Advisories, DSA 874-1 & 876-1, October 27, 2005**
MyBB Group MyBulletinBoard 1.0 PR2, RC4	An SQL injection vulnerability has been reported in 'Usercp.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	MyBulletinBoard SQL Injection CVE-2005-3326	Medium	Security Focus, Bugtraq ID: 15204, October 26, 2005
Network Appliance Data ONTAP 7.0, 6.5, 6.4	A vulnerability has been reported when handling iSCSI authentication requests, which could let a remote malicious user bypass authentication. Updates available at: http://now.netapp.com/ NOW/cgi-bin/ software Currently we are not aware of any exploits for this vulnerability.	Network Appliance iSCSI Authentication Bypass CVE-2005-3327	Medium	Secunia Advisory: SA17321, October 25, 2005
Nuked-Klan Nuked-Klan 1.7	Several vulnerabilities have been reported: Cross-Site Scripting vulnerabilities have been reported in the 'search,' 'guestbook,' 'textbook,' and 'forum' modules due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and SQL injection vulnerabilities were reported due to insufficient sanitization of the 'forum_id,' 'thread_id,' 'link_id,' 'artid,' and 'dl_id' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Nuked Klan Multiple Cross-Site Scripting & SQL Injection CVE-2005-3305	Medium	Secunia Advisory: SA17304, October 25, 2005
Oracle Corporation JD Edwards EnterpriseOne 8.x, OneWorld 8.x; Oracle Application Server 10g, Collaboration Suite Release 1, 2, Database 8.x, Database Server 10g, Developer Suite 10g, E-Business Suite 11i, Enterprise Manager 10.x, 9.x, Oracle9i Application Server, Oracle9i Database Enterprise Edition, Oracle9i Database Standard Edition, Workflow 11.5.9 .5, 11.5.1; PeopleSoft Enterprise Customer Relationship Management (CRM) 8.x, EnterpriseOne Applications 8.x	85 vulnerabilities have been reported in various Oracle products. Some have an unknown impact, and others can be exploited to conduct SQL injection attacks, Cross-Site Scripting attacks, or potentially to compromise a vulnerable system. Patch information available at: http://www.oracle.com/ technology/deploy/ security/pdf/cpuoct2005.html Currently we are not aware of any exploits for these vulnerabilities.	Oracle October Security Update	High	Oracle Critical Patch Update, October 18, 2005 Technical Cyber Security Alert TA05-292A, October 19, 2005 US-CERT VU#210524 **US-CERT VU#865948**, **VU#890940**, **VU#376756**, **VU#171364**, **VU#512716,** **VU#150508**, **VU#609340**, **VU#265700**, **VU#449444**

Paros Paros 3.2.5	A vulnerability has been reported in the built-in 'hsqldb' database due to a default password, which could let a remote malicious bypass authentication procedures. Upgrade available at: http://prdownloads.sourceforge.net/paros/paros-3.2.6-unix.zip There is no exploit code required.	Paros 'HSQLDB' Remote Authentication Bypass CVE-2005-3280	Medium	Security Focus, Bugtraq ID: 15141, October 19, 2005
PHP Group PHP 5.0.5, 4.4.0	A vulnerability has been reported in the 'open_basedir' directive due to the way PHP handles it, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ **Trustix:** **http://http.trustix.org/pub/trustix/updates/** There is no exploit code required.	PHP 'Open_BaseDir' Information Disclosure CVE-2005-3054	Medium	Security Focus, Bugtraq ID: 14957, September 27, 2005 Ubuntu Security Notice, USN-207-1, October 17, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005**
PHP iCalendar PHP iCalendar 2.0.1, 2.0 c, 2.0 b, 2.0 a2	A vulnerability has been reported in 'Default_View' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary remote PHP code. No workaround or patch available at time of publishing. There is no exploit code required.	PHP ICalendar Remote File Include	Medium	Security Focus, Bugtraq ID: 15193, October 25, 2005
phpBB Group phpBB 2.0.17	A vulnerability has been reported in avatar upload handling due to an input validation error, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	phpBB Avatar Upload Handling Input Validation CVE-2005-3310	Medium	Security Focus, Bugtraq ID: 15170, October 22, 2005
PHPNuke NukeFix 3.1 for V7.8	A Directory Traversal vulnerability has been reported in the NukeFixes Addon due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	PHP-Nuke Modules.PHP NukeFixes Addon Remote Directory Traversal CVE-2005-3281	Medium	Secunia Advisory: SA17218, October 20, 2005
Platinum DboardGear	SQL injection vulnerabilities have been reported in 'buddy.php,' 'u2a.php,' and 'Theme Import' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Platinum DBoardGear Multiple SQL Injection	Medium	Security Focus, Bugtraq ID: 15174 & 15194, October 24 & 25, 2005
PunBB PunBB 1.1.2-1.1.5	A vulnerability has been reported in 'common.php' which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PunBB 'Common.PHP' Remote File Include CVE-2005-3328	Medium	Security Focus, Bugtraq ID: 15175, October 24, 2005
Skype Technologies Skype 1.4.0.83, 1.1.0.0	Several buffer overflow vulnerabilities have been reported: a vulnerability was reported when handling Skype-specific URI types due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when handling VCARD imports due to a boundary error, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported when handling certain unspecified Skype client network traffic due to a boundary error, which could let a remote malicious user cause a remote Denial of Service. Upgrades available at: http://www.skype.com/products/skype/ Currently we are not aware of any exploits for these vulnerabilities.	Skype Technologies Skype Multiple Buffer Overflows CVE-2005-3265 CVE-2005-3267	High	Skype Technologies Security Advisory, SKYPE-SB/2005-002 & SKYPE-SB/2005-003, October 25, 2005 US-CERT VU#905177, VU#930345, VU#668193

Snoopy Snoopy 1.2	A vulnerability has been reported in the '_httpsrequest()' function due to insufficient validation of user-supplied input before making a PHP exec() call, which could let a remote malicious user execute arbitrary commands. Update available at: http://sourceforge.net/project/showfiles.php?group_id=2091 There is no exploit code required; however, a Proof of Concept exploit has been published.	Snoopy Input Validation CVE-2005-3330	Medium	SEC-CONSULT Security Advisory 20051025-0, October 25, 2005
Splatt Forum Splatt Forum 3.0-3.2	A vulnerability has been reported because the administrative logon process may be bypassed, which could let a remote malicious user bypass authentication procedures. The vendor has released version 4.0 to address this issue. There is no exploit code required.	Splatt Forums Remote Administrative Logon Bypass CVE-2005-3282	Medium	Security Focus, Bugtraq ID: 15152, October 20, 2005
Sun Micro-systems, Inc. Java Web Start 1.x, Sun Java JDK 1.5.x, 1.4.x, Sun Java JRE 1.4.x, 1.5.x	Several vulnerabilities have been reported: a vulnerability was reported due to an unspecified error which could let malicious untrusted applications execute arbitrary code; and a vulnerability was reported due to an unspecified error which could let a malicious untrusted applets execute arbitrary code. Upgrades available at: http://java.sun.com/j2se/1.5.0/index.jsp http://java.sun.com/j2se/1.4.2/download.html Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-current/ SUSE: ftp://ftp.SUSE.com/pub/SUSE HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBUX01214 **HP:** **http://h20000.www2.hp.com/bizsupport/TechSupport/** Currently we are not aware of any exploits for these vulnerabilities.	Java Web Start / Sun JRE Sandbox Security Bypass CVE-2005-1973 CVE-2005-1974	High	Sun(sm) Alert Notification, 101748 & 101749, June 13, 2005 Slackware Security Advisory, SSA:2005-170-01, June 20, 2005 SUSE Security Announcement, SUSE-SA:2005:032, June 22, 2005 HP Security Bulletin, HPSBUX01214, August 29, 2005 HP Security Bulletin, HPSBMA01234, October 19, 2005
TikiWiki Project TikiWiki 1.9.1, 1.8.5	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of unspecified user-input, which could let la remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/tikiwiki/tikiwiki-1.9.1.1.tar.gz There is no exploit code required.	TikiWiki Unspecified Cross-Site Scripting CVE-2005-3283	Medium	Security Tracker Alert ID: 1015087, October 20, 2005
TriggerTG TClanPortal 3.0	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	TriggerTG TClanPortal SQL Injection	Medium	Security Focus, Bugtraq ID: 15173, October 24, 2005
XMail XMail 1.21	A buffer overflow vulnerability has been reported in the 'AddressFromAtPtr()' function due to a boundary error when copying the hostname portion of an e-mail address to a 256-byte buffer, which could let a malicious user execute arbitrary code.	XMail Command Line Buffer Overflow CVE-2005-2943	High	Security Tracker Alert ID: 1015055, October 13, 2005 **Security Focus, Bugtraq ID: 15103, October 22, 2005**

	Upgrade available at: http://www.xmailserver.org/ **An exploit script has been published.**			
Xoops Xoops 2.0.12 JP & prior, 2.0.13.1 & prior, 2.2.3 RC1 & prior	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient sanitization of 'XOOPS Code' tags before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'newbb' forum module due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.jp/xoops/17125/xoops-2.0.13a-JP.tar.gz There is no exploit code required.	Xoops Arbitrary Script Execution CVE-2005-2338	Medium	Secunia Advisory: SA17300, October 25, 2005
Yiff Sound Systems Yiff Sound Systems 2.14.5	A vulnerability has been reported in the 'yplay' application due to a failure to verify file permissions before playing back user-specified files, which could let a malicious user bypass certain security restrictions. No workaround or patch available at time of publishing. There is no exploit code required.	Yiff-Server File Permission Bypass CVE-2005-3268	Medium	Secunia Advisory: SA17242, October 19, 2005
Zomplog Zomplog 3.4, 3.3	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'detail.php' due to insufficient sanitization of the 'id' parameter, and in 'get.php' and 'index.php' due to insufficient sanitization of the 'catid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'detail.php' due to insufficient sanitization of the 'name' parameter, in the 'get.php' parameter due to insufficient sanitization of the 'username' parameter, and in 'index.php' due to insufficient sanitization of the 'search' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Zomplog Cross-Site Scripting CVE-2005-3308 CVE-2005-3309	Medium	Nightmare TeAmZ Advisory 011, October 20, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **VoIP security threats defined:** The VoIP Security Alliance (VoIPSA) has published their first document that contains a laundry list of security threats. The document, which defines security threats facing VoIP deployments, raises awareness on a technology that is becoming more and more mainstream. While threats such as caller ID spoofing, Denial of Service attacks and eavesdropping attacks have been known for some time, the VoIPSA public report identifies many additional areas where VoIP technology remains vulnerable. Source: http://www.securityfocus.com/brief/23.
- **Face recognition security comes to mobiles:** Oki Electric Industry has developed Face Sensing Engine software that decodes facial images and restricts phone access to everyone except the registered user. Source: http://www.vnunet.com/vnunet/news/2144460/face-recognition-mobiles.
- **US firms rush to embrace VoIP:** According to a poll by Qwest Communications of US-based IT professionals. US companies anticipate saving 40 per cent on telecommunication costs as a result of implementing voice over IP (VoIP). They found that 100 per cent of respondents plan to install new or additional VoIP services within the next year. Source: http://www.vnunet.com/vnunet/news/2144654/firms-rush-roll-voip.
- **Voice Over WLAN To Triple In By 2007: Report:** According to a report from Infonetics Research, voice over wireless local area network (VoWLAN) adoption will triple over the next two years. This reflects the overall trend of WLAN adoption. By 2007, 31% of companies surveyed for the study will have implemented the technology, compared to 10% today. Source: http://www.mobilepipeline.com/news/172303117;jsessionid=3XKESATIGIDGQQSNDBGCKH0CJUMEKJVN.

Wireless Vulnerabilities

- **Linux Kernel Bluetooth Signed Buffer Index vulnerability:** Another exploit script has been published.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script	Script name	Workaround or	Script Description

(Reverse Chronological Order)		Patch Available	
October 26, 2005	dietsniff-0.3.tar.bz2	N/A	A tiny tool for analyzing traffic on a network when a small and especially static sniffer is required.
October 26, 2005	diit_1-2.tgz	N/A	A tool that can hide a message inside a 24-bit color image so that knowing how it was embedded, or performing statistical analysis, does not make it any easier to find the concealed information.
October 26, 2005	MyBB_SQL.pl	No	Proof of Concept exploit script for the MyBulletinBoard SQL Injection vulnerability.
October 26, 2005	scapy-1.0.1.tar.gz	N/A	A powerful interactive packet manipulation tool, packet generator, network scanner, network discovery tool, and packet sniffer.
October 26, 2005	Zomplog.txt	No	Proof of Concept exploit for the Zomplog Cross-Site Scripting & SQL Injection vulnerabilities.
October 25, 2005	dis.c.txt	N/A	A port of z0mbie's Length-Disassembler-Engine (LDE) into VC7++ assembler syntax that now fits in one naked function. This is useful for hooking and code injection techniques.
October 25, 2005	NetFlowAnalyzer4.txt	No	Proof of Concept exploit for the NetFlow Analyzer Cross-Site Scripting vulnerability.
October 25, 2005	snort_bo_ping.pm THCsnortbo.c	Yes	Proof of Concept exploit scripts for the Snort Back Orifice Preprocessor Remote Buffer Overflow vulnerability.
October 24, 2005	nk_1.7.exploit.pl	No	Proof of Concept exploit for the PHP-Nuke SQL Injection Vulnerabilities.
October 24, 2005	phpnuke_78_xpl.php SA025-PHPNuke.txt	No	Proof of Concept exploits for the PHPNuke Multiple Modules SQL Injection Vulnerabilities.
October 24, 2005	TClanPortal_sql_inj.pl	No	Proof of Concept exploit for the TriggerTG TClanPortal Index.PHP SQL Injection vulnerability.
October 22, 2005	xmail-1.21.sendmail.local.exploit.c	Yes	Script that exploits the XMail Command Line Buffer Overflow vulnerability.
October 21, 2005	Comersus-BackOffice.txt	No	Exploitation details for the Comersus BackOffice Plus Cross-Site Scripting vulnerability.
October 21, 2005	ethereal-0.10.13.tar.bz2	N/A	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
October 21, 2005	Punbb-1.2.8.txt	No	Proof of Concept exploit for the Punbb 'Search.php' SQL Injection vulnerability.
October 21, 2005	typsoft-1.11.txt	No	Proof of Concept exploit for the TYPSoft FTP Server RETR Denial of Service Vulnerability.
October 20, 2005	ethereal_slimp3_bof.py	Yes	A Denial of Service exploit for the SLIMP3 protocol dissector vulnerability.
October 24, 2005	ong_bak_0.9.c	Yes	Exploit script for the Linux Kernel Bluetooth Signed Buffer Index vulnerability.

[back to top]

Trends

- **Extortion virus makes rounds in Russia:** According to a weblog published by Kaspersky Lab Ltd., two new versions of a virus first reported in May are staging renewed attacks against computers in Russia, encrypting files and then extorting money from victims to decode the files. The viruses, called JuNy.A and JuNy.B, search for more than 100 file types by extension. Source: http://www.computerworld.com/securitytopics/security/virus/story/0,10801,105706,00.html?source=NLT_PM&nid=10570.
- **GAO: Agencies face collaboration barriers:** According to a report issued from the Government Accountability Office, agencies face several barriers to collaboration, such as competing missions, incompatible systems and concerns over turf and resources. GAO has outlined eight practices which evolved from the agencies review of a federal programs, that would improve coordination among federal agencies. Source: http://www.fcw.com/article91199-10-25-05-Web
- According to F-Secure, a new botnet, Mocbot, is circulating. This botnet client has been spread using the MS05-047 vulnerability. The vulnerability can be exploited via 139/TCP and 445/TCP. The existence of a file called wudpcom.exe in the SYSTEM directory is a symptom of an infection. Source: http://www.f-secure.com/weblog/archives/archive-102005.html#00000685.
- **Hackers, Scammers Hide Malicious JavaScript On Web Sites:** According to a the senior directory of security and research at Websense, hackers and scammers are using a new technique to hide malicious JavaScript on compromised or criminal sites. A family of obfuscation routines with the umbrella name of "JS/Wonka" has spread wildly in the last few weeks. Source: http://informationweek.com/story/showArticle.jhtml?articleID=172302840.
- **Robot Wars – How Botnets Work:** One of the most common and efficient DDoS attack methods is based on using hundreds of zombie hosts. Zombies are usually controlled and managed via IRC networks, using so-called botnets. Source: http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection.

It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
3	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
4	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
5	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
6	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
7	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
8	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
9	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
10	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.

Table updated October 24, 2005

[back to top]

Last updated October 27, 2005