

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

- Windows Operating Systems
  - [ASP Fast Forum Cross Site Scripting](#)
  - [Asus VideoSecurity Online Directory Traversal or Information Disclosure](#)
  - [Comersus BackOffice Multiple Vulnerabilities](#)
  - [F-Secure Anti-Virus for Exchange and Internet Gatekeeper Directory Traversal](#)
  - [GraphOn GO-Global For Windows Denial of Service or Arbitrary Code Execution](#)
  - [Hyper Estraier Information Disclosure](#)
  - [\*\*Microsoft Internet Explorer Arbitrary Code Execution \(Updated\)\*\*](#)
  - [\*\*Microsoft Internet Explorer Arbitrary Code Execution \(Updated\)\*\*](#)
  - [InnerMedia DynaZip Arbitrary Code Execution](#)
  - [Serv-U FTP Server Denial of Service](#)
  - [RockLiffe MailSite Express WebMail Multiple Vulnerabilities](#)
  - [Techno Dreams Multiple Product SQL Injection](#)
- UNIX / Linux Operating Systems
  - [Apple Mac OS X Security Update](#)
  - [BeMoore Software News2Net SQL Injection](#)
  - [\*\*CVS 'Cvsbug.In' Script Insecure Temporary File Creation \(Updated\)\*\*](#)
  - [\*\*FreeBSD IPsec AES-XCBC-MAC Algorithm Unauthorized Connections \(Updated\)\*\*](#)
  - [IBM AIX 'chcon' Buffer Overflow](#)
  - [\*\*Info-ZIP UnZip File Permission Modification \(Updated\)\*\*](#)
  - [Luca Deri NTop Insecure Temporary File Creation](#)
  - [MailWatch for MailScanner SQL Injection & Directory Traversal](#)
  - [Multiple Vendors Apache Authentication Bypassing](#)
  - [\*\*Multiple Vendors Linux Kernel IPV6 Denial of Service \(Updated\)\*\*](#)
  - [\*\*Zlib Compression Library Buffer Overflow \(Updated\)\*\*](#)
  - [\*\*Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service \(Updated\)\*\*](#)
  - [Multiple Vendors GDB Multiple Vulnerabilities \(Updated\)](#)
  - [\*\*Multiple Vendors GNOME-DB LibGDA Multiple Format String \(Updated\)\*\*](#)
  - [Multiple Vendors GNUMP3d Cross-Site Scripting or Directory Traversal](#)
  - [\*\*Multiple Vendors Linux Kernel Denial of Service & Information Disclosure \(Updated\)\*\*](#)
  - [\*\*Multiple Vendors Linux Kernel Denials of Service \(Updated\)\*\*](#)
  - [\*\*Multiple Vendors OpenSSL Insecure Protocol Negotiation \(Updated\)\*\*](#)
  - [Multiple Vendors Pluggable Authentication Modules Security Bypassing](#)
  - [\*\*Multiple Vendors NetPBM Buffer Overflow \(Updated\)\*\*](#)
  - [\*\*Multiple Vendors XFree86 Pixmap Allocation Buffer Overflow \(Updated\)\*\*](#)
  - [OpenVPN Client Remote Format String & Denial of Service](#)
  - [\*\*SCO UnixWare Portmapper Denial of Service \(Updated\)\*\*](#)
  - [Sun Solaris Cross-Site Scripting](#)
  - [Sun Java System Communications Express Information Disclosure](#)
  - [\*\*Sun Solaris Runtime Linker 'LD\\_AUDIT' Elevated Privileges \(Updated\)\*\*](#)
  - [\*\*Todd Miller Sudo Local Elevated Privileges \(Updated\)\*\*](#)
  - [\*\*Uim Elevated Privileges \(Updated\)\*\*](#)
  - [\*\*Xloadimage NIFF Image Buffer Overflow \(Updated\)\*\*](#)
- Multiple Operating Systems
  - [Simple PHP Blog Cross-Site Scripting](#)
  - [ATutor Multiple Vulnerabilities](#)
  - [Cisco Management Center for IPS Sensors Signature Disable](#)
  - [\*\*codetosell ViArt Shop Enterprise Cross-Site Scripting \(Updated\)\*\*](#)
  - [eyeOS Script Insertion & Information Disclosure](#)
  - [First4Internet XCP Content Management Security Bypass](#)
  - [gCards SQL Injection](#)
  - [Hasbani Web Server Denial of Service](#)
  - [HP OpenVMS Denial of Service](#)
  - [Invision Gallery Image Input Validation](#)
  - [Invision Gallery SQL Injection](#)
  - [Jed Wing CHM Lib '\\_chm\\_find\\_\\_in\\_PMGL Remote Buffer Overflow](#)
  - [\*\*Mantis Multiple Vulnerabilities \(Updated\)\*\*](#)
  - [\*\*Multiple Vendors Telnet Client 'slc\\_add\\_reply\(\)' & 'env\\_opt\\_add\(\)' Buffer Overflows \(Updated\)\*\*](#)
  - [\*\*Multiple Vendors CVS Multiple Vulnerabilities \(Updated\)\*\*](#)

- [Ethereal Denial of Service](#)
- [Multiple Vendors Ethereal Multiple Protocol Dissector Vulnerabilities \(Updated\)](#)
- [Multiple Vendors Anti-Virus Magic Byte Detection Evasion \(Updated\)](#)
- [Multiple Vendors Lynx 'HTrijs\(\)' NNTP Remote Buffer Overflow \(Updated\)](#)
- [Novell ZENworks Patch Management SQL Injection](#)
- [OaBoard SQL Injection](#)
- [PBLang Multiple Cross-Site Scripting Vulnerabilities](#)
- [PHP Advanced Transfer Manager Unauthorized Access](#)
- [PHP 'Open BaseDir' Information Disclosure \(Updated\)](#)
- [PHP Multiple Vulnerabilities](#)
- [phpBB Deregistration Global Variables](#)
- [PHPCafe Tutorial Manager SQL Injection](#)
- [phpESP Cross-Site Scripting & SQL Injection](#)
- [PHP-Nuke Cross-Site Scripting](#)
- [Ringtail CaseBook Cross-Site Scripting & Information Disclosure](#)
- [Snitz Forum Cross-Site Scripting](#)
- [Subdreamer SQL Injection](#)
- [Thomas Rybak MG2 Authentication Bypassing](#)
- [TikiWiki Unspecified Cross-Site Scripting \(Updated\)](#)
- [Woltlab Burning Board SQL Injection](#)

[Wireless](#)

[Recent Exploit Scripts/Techniques](#)

[Trends](#)

[Viruses/Trojans](#)

## 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
ASP Fast Forum	A vulnerability has been reported in ASP Fast Forum 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, Proof of Concept exploits have been published.	ASP Fast Forum Cross Site Scripting  <a href="#">CVE-2005-3422</a>	Medium	Secunia, Advisory: SA17387, October 31, 2005
Asus VideoSecurity Online 3.5	A vulnerability has been reported in VideoSecurity Online that could let remote malicious users traverse directories or disclose information.  No workaround or patch available at time of publishing.  There is no exploit code required.	Asus VideoSecurity Online Directory Traversal or Information Disclosure	Medium	Security Focus, ID: 15281, November 2, 2005
Comersus BackOffice	Multiple input validation vulnerabilities have been reported in BackOffice that could let remote malicious users disclose sensitive information, perform SQL injection, or conduct Cross-Site Scripting.  No workaround or patch available at time of publishing.  There is no exploit code required; however, Proof of	Comersus BackOffice Multiple Vulnerabilities  <a href="#">CVE-2005-3397</a>	Medium	Security Focus, ID: 15251, October 31, 2005

	Concept exploits have been published.			
F-Secure Anti-Virus for Microsoft Exchange 6.40 and Internet Gatekeeper 6.40, 6.41, 6.42	A vulnerability has been reported in F-Secure Anti-Virus for Microsoft Exchange and Internet Gatekeeper that could let local malicious users traverse directories.  Vendor fix available: <a href="http://www.f-secure.com/security/fsc-2005-2.shtml">http://www.f-secure.com/security/fsc-2005-2.shtml</a>  There is no exploit code required.	F-Secure Anti-Virus for Exchange and Internet Gatekeeper Directory Traversal  <a href="#">CVE-2005-3468</a>	Medium	Secunia, Advisory: SA17361, November 2, 2005
GraphOn GoGlobal for Windows prior to 3.1.0.3270	A buffer overflow vulnerability has been reported in GraphOn GoGlobal for Windows that could let a remote malicious user execute arbitrary code or cause a Denial of Service.  No workaround or patch available at time of publishing.  A Proof of Concept exploit has been published.	GraphOn GO-Global For Windows Denial of Service or Arbitrary Code Execution	High	Security Focus, ID: 15285, November 2, 2005
Hyper Estraier 1.0, 1.0.1	A vulnerability has been reported in Hyper Estraier that could let remote malicious users disclose information.  Upgrade to version 1.0.2: <a href="http://hyperestraier.sourceforge.net/hyperestraier-1.0.2.tar.gz">http://hyperestraier.sourceforge.net/hyperestraier-1.0.2.tar.gz</a>  There is no exploit code required.	Hyper Estraier Information Disclosure  <a href="#">CVE-2005-3421</a>	Medium	Security Focus, ID: 15236, October 28, 2005
Microsoft Internet Explorer	A memory corruption vulnerability has been reported in Internet Explorer COM Object instantiation that could let remote malicious users execute arbitrary code.  Vendor fix available: <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp</a>  <b>V1.3 Issues discovered in in the security update: Microsoft Knowledge Base Article 906294.</b>  A Proof of Concept exploit has been published.	Microsoft Internet Explorer Arbitrary Code Execution  <a href="#">CVE-2005-1990</a>	High	Microsoft Security Bulletin MS05-038, August 9, 2005  <a href="#">US-CERT VU#959049</a>  <b>Microsoft Security Bulletin MS05-038 V1.3, November 2, 2005</b>
Microsoft Internet Explorer 5.01, 5.5, 6.0	A vulnerability has been reported in Internet Explorer that could let remote malicious users execute arbitrary code.  Vendor fix available: <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-052.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-052.msp</a>  <b>V1.3 Issues discovered in in the security update: Microsoft Knowledge Base Article 909889.</b>  Avaya: <a href="http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf">http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf</a>  An exploit has been published.	Microsoft Internet Explorer Arbitrary Code Execution  <a href="#">CVE-2005-2127</a>	High	Microsoft, Security Bulletin MS05-052, October 11, 2005  Technical Cyber Security Alert TA05-284A, October 11, 2005  Avaya, ASA-2005-214, October 11, 2005  <a href="#">USCERT, VU#680526, VU#959049, VU#740372, VU#898241</a>  <b>Microsoft, Security Bulletin MS05-052 V1.3, November 2, 2005</b>
Multiple Vendors Real Networks RealPlayer 10.5, v6.0.12.1053, v6.0.12.1040, 10.5 Beta v6.0.12.1016, 10.0 BETA, 10.0, v6.0.12.690, RealOne Player 2.0, 1.0; InnerMedia DynaZip Library 3.0 .0.14, 5.00.00-5.00.03; CheckMark Software Inc. MultiLedger 7.0, 6.0.3, CheckMark Payroll 3.9.1-3.9.6	A buffer overflow vulnerability has been reported in DynaZip that could let remote malicious users execute arbitrary code.  RealPlayer/RealOne: Fixes are available via the "Check for Update" feature.  DynaZip: Update to version 5.00.04 or later.  DynaZip Max: Update to version 6.00.01 or later.  CheckMark Software: <a href="http://www.checkmark.com/support/patch_win_pr.php">http://www.checkmark.com/support/patch_win_pr.php</a>  An exploit has been published.	InnerMedia DynaZip Arbitrary Code Execution  <a href="#">CVE-2004-1094</a>	High	Security Focus, ID: 11555, October 27, 2005  <a href="#">US-CERT VU#582498</a>
RhinoSoft Serv-U FTP Server	A vulnerability has been reported in Serv-U FTP Server that could let remote malicious users cause a Denial of Service.  Vendor upgrade available:	Serv-U FTP Server Denial of Service  <a href="#">CVE-2005-3467</a>	Low	Secunia, Advisory: SA17409, November 2, 2005

<http://www.serv-u.com/dn.asp>

There is no exploit code required.

<p>RockLiffe</p> <p>Mailsite Express WebMail prior to 6.1.22</p>	<p>Multiple vulnerabilities have been reported in MailSite Express WebMail that could let remote malicious users disclose information, arbitrary file control, or execute arbitrary code.</p> <p>A vendor fix is available:  <a href="http://www.rockliffe.com/userroom/download.asp">http://www.rockliffe.com/userroom/download.asp</a></p> <p>There is no exploit code required.</p>	<p>RockLiffe MailSite Express WebMail Multiple Vulnerabilities</p> <p><a href="#">CVE-2005-3428</a>  <a href="#">CVE-2005-3429</a>  <a href="#">CVE-2005-3430</a>  <a href="#">CVE-2005-3431</a></p>	<p>Medium</p>	<p>Security Focus, ID: 15231, 15230, October 28, 2005</p>
<p>Techno Dreams</p> <p>Announcement, Guest Book, Mailing List, Web Directory</p>	<p>A vulnerability has been reported in Techno Dreams Announcement, Guest Book, Mailing List, and Web Directory that could let remote malicious users perform SQL injection.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>Techno Dreams Multiple Product SQL Injection</p> <p><a href="#">CVE-2005-3383</a>  <a href="#">CVE-2005-3384</a>  <a href="#">CVE-2005-3385</a>  <a href="#">CVE-2005-3386</a></p>	<p>Medium</p>	<p>Secunia, Advisory: SA17354, October 27, 2005</p>

[back to top](#)

UNIX / Linux Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
<p>Apple</p> <p>Apple Mac OS X Server 1-4-10.4.2, Server 10.3-10.3.9, 10.2-10.2.8, 10.0-10.1.5, Mac OS X 1-4-10.4.2, 10.3-10.3.9, 10.2-10.2.8, 10.1-10.1.5, 10.0-10.0.4</p>	<p>Multiple vulnerabilities have been reported: a misleading file ownership display vulnerability was reported, which could result in a false sense of security; a software update failure vulnerability was reported, which could potentially result in a failure to install critical security fixes; a group membership alteration issue was reported, which could result in unauthorized access; an information disclosure vulnerability was reported in Keychain, which could let a malicious user obtain sensitive information; and multiple information disclosure vulnerabilities were reported in the kernel, which could potentially let malicious users obtain sensitive information.</p> <p>Update information available at:  <a href="http://docs.info.apple.com/article.html?artnum=302763">http://docs.info.apple.com/article.html?artnum=302763</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>Apple Mac OS X Security Update</p> <p><a href="#">CVE-2005-2749</a>  <a href="#">CVE-2005-2750</a>  <a href="#">CVE-2005-2751</a>  <a href="#">CVE-2005-2739</a>  <a href="#">CVE-2005-1126</a>  <a href="#">CVE-2005-1406</a>  <a href="#">CVE-2005-2752</a></p>	<p>Medium</p>	<p>Apple Security Advisory, APPLE-SA-2005-10-31, October 31, 2005</p>
<p>BeMoore Software</p> <p>News2Net 3.x</p>	<p>An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'category' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>News2Net SQL Injection</p> <p><a href="#">CVE-2005-3469</a></p>	<p>Medium</p>	<p>Secunia Advisory: SA17396, November 2, 2005</p>

<p>CVS</p> <p>CVS 1.12.7-1.12.12, 1.12.5, 1.12.2, 1.12.1, 1.11.19, 1.11.17</p>	<p>A vulnerability has been reported in the 'cvsbug.in' script due to the insecure creation of temporary files, which could let a malicious user cause data loss or a Denial of Service.</p> <p>Fedora:  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>Trustix:  <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p>FreeBSD:  <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:20/cvsbug.patch">ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:20/cvsbug.patch</a></p> <p>SGI:  <a href="ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/">ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/</a></p> <p>Debian:  <a href="http://security.debian.org/pool/updates/main/c/cvs/">http://security.debian.org/pool/updates/main/c/cvs/</a></p> <p><a href="http://security.debian.org/pool/updates/main/g/gcvs/">http://security.debian.org/pool/updates/main/g/gcvs/</a></p> <p>FreeBSD:  <a href="ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:20.cvsbug.asc">ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:20.cvsbug.asc</a></p> <p><b>NetBSD:</b>  <a href="http://arkiv.netbsd.se/?ml=netbsd-announce&amp;a=2005-10&amp;m=1435804">http://arkiv.netbsd.se/?ml=netbsd-announce&amp;a=2005-10&amp;m=1435804</a></p> <p>There is no exploit code required.</p>	<p>CVS 'Cvsbug.In' Script Insecure Temporary File Creation</p> <p><a href="#">CVE-2005-2693</a></p>	<p>Low</p>	<p>Fedora Update Notifications  FEDORA-2005-790 &amp; 791, August 23, 2005</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2005-0045, August 26, 2005</p> <p>RedHat Security Advisory, RHSA-2005:756-3, September 6, 2005</p> <p>SGI Security Advisory, 20050901-01-U, September 7, 2005</p> <p>FreeBSD Security Advisory, FreeBSD-SA-05:20, September 7, 2005</p> <p>Debian Security Advisories, DSA 802-1 &amp; 806-1, September 7 &amp; 9, 2005</p> <p>FreeBSD Security Advisory, FreeBSD-SA-05:20, September 9, 2005</p> <p><b>NetBSD Security Update, November 1, 2005</b></p>
<p>FreeBSD</p> <p>IPSec AES-XCBC-MAC Algorithm V5.3, 5.4, 6.0Beta</p>	<p>A vulnerability has been reported in FreeBSD's IPSec AES-XCBC-MAC Algorithm, which could allow for incorrect key usage, and consequently allow remote malicious users to connect via unauthorized IPSec connections.</p> <p>A vendor patch is available:  <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:19/">ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:19/</a></p> <p><b>NetBSD:</b>  <a href="http://www.kame.net/dev/cvsweb2.cgi/kame/kame/sys/netinet6/ah_aesxcbcm.ac.c.diff?r1=1.7&amp;r2=1.8">http://www.kame.net/dev/cvsweb2.cgi/kame/kame/sys/netinet6/ah_aesxcbcm.ac.c.diff?r1=1.7&amp;r2=1.8</a></p> <p>There is no exploit code required.</p>	<p>FreeBSD IPSec AES-XCBC-MAC Algorithm Unauthorized Connections</p> <p><a href="#">CVE-2005-2359</a></p>	<p>Medium</p>	<p>FreeBSD Security Advisory  FreeBSD-SA-05:19, July 27, 2005</p> <p><b>Security Focus, Bugtraq ID: 14394, November 1, 2005</b></p>
<p>IBM</p> <p>AIX 5.3 L, 5.3, 5.2.2, 5.2 L, 5.2, 5.1 L, 5.1</p>	<p>A buffer overflow vulnerability has been reported in the 'chcon' command. The impact was not specified</p> <p>Vendor patch available:  <a href="http://www-03.ibm.com/servers/eserver/support/pseries/aixfixes.html">http://www-03.ibm.com/servers/eserver/support/pseries/aixfixes.html</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>IBM AIX 'chcon' Buffer Overflow</p> <p><a href="#">CVE-2005-3396</a></p>	<p>Not Specified</p>	<p>IBM, IY78241, IY78253, October 28, 2005</p>
<p>Info-ZIP</p> <p>UnZip 5.52</p>	<p>A vulnerability has been reported due to a security weakness when extracting an archive to a world or group writeable directory, which could let a malicious user modify file permissions.</p>	<p>Info-ZIP UnZip File Permission Modification</p> <p><a href="#">CVE-2005-2475</a></p>	<p>Medium</p>	<p>Security Focus, 14450, August 2, 2005</p> <p>Fedora Update Notification,</p>

	<p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/</a></p> <p>SCO: <a href="ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.39/507">ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.39/507</a></p> <p>Ubuntu: <a href="http://security.ubuntu.com/ubuntu/pool/main/u/unzip/">http://security.ubuntu.com/ubuntu/pool/main/u/unzip/</a></p> <p>Trustix: <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p><b>Mandriva:</b> <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p>There is no exploit code required.</p>			<p>FEDORA-2005-844, September 9, 2005</p> <p>SCO Security Advisory, SCOSA-2005.39, September 28, 2005</p> <p>Ubuntu Security Notice, USN-191-1, September 29, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0053, September 30, 2005</p> <p><b>Mandriva Linux Security Update Advisory, MDKSA-2005:197, October 26, 2005</b></p>
Luca Deri ntop 3.1	<p>A vulnerability has been reported in 'ntopinitparms' due to the insecure creation of a temporary file, which could let a remote malicious user create/overwrite arbitrary files.</p> <p>Upgrade available at: <a href="http://prdownloads.sourceforge.net/ntop/ntop-3.2.tgz?download">http://prdownloads.sourceforge.net/ntop/ntop-3.2.tgz?download</a></p> <p>There is no exploit code required.</p>	<p>NTop Insecure Temporary File Creation</p> <p><a href="#">CVE-2005-3387</a></p>	Medium	<p>Security Focus, Bugtraq ID: 15242, October 31, 2005</p>
MailWatch for MailScanner MailWatch for MailScanner 1.0.2	<p>Several vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of the 'authenticate()' function before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Directory Traversal vulnerability was reported in the ruleset view. The impact was not specified.</p> <p>Updates available at: <a href="http://sourceforge.net/project/showfiles.php?group_id=87163">http://sourceforge.net/project/showfiles.php?group_id=87163</a></p> <p>There is no exploit code required.</p>	<p>MailWatch for MailScanner SQL Injection &amp; Directory Traversal</p> <p><a href="#">CVE-2005-3470</a> <a href="#">CVE-2005-3471</a></p>	Medium	<p>Secunia Advisory: SA17405, November 2, 2005</p>
Multiple Vendors Apache Mod_Auth_Shadow 1.0 to 1.4, 2.0	<p>A vulnerability has been reported in Apache, Mod_Auth_Shadow, that could let remote malicious users bypass authentication.</p> <p>Upgrades available at: <a href="http://prdownloads.sourceforge.net/mod-auth-shadow/mod_auth_shadow-1.5.tar.gz?download">http://prdownloads.sourceforge.net/mod-auth-shadow/mod_auth_shadow-1.5.tar.gz?download</a></p> <p>Debian: <a href="http://security.debian.org/pool/updates/main/m/mod-auth-shadow/">http://security.debian.org/pool/updates/main/m/mod-auth-shadow/</a></p> <p>Mandriva: <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p>There is no exploit code required.</p>	<p>Apache Authentication Bypassing</p> <p><a href="#">CVE-2005-2963</a></p>	Medium	<p>Security Focus, ID: 15224, October 27, 2005</p> <p>Debian Security Advisory, DSA 844-1, October 5, 2005</p> <p>Mandriva Linux Security Advisory MDKSA-2005:200, October 27, 2005</p>
Multiple Vendors Linux Kernel Linux kernel 2.6- 2.6.14	<p>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.</p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p><b>Upgrades available at:</b></p>	<p>Linux Kernel IPV6 Denial of Service</p> <p><a href="#">CVE-2005-2973</a></p>	Low	<p>Secunia Advisory: SA17261, October 21, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-1007 &amp; 1013, October 20, 2005</p> <p><b>Security Focus, Bugtraq</b></p>

[http://kernel.org/  
pub/linux/kernel/  
v2.6/linux-  
2.6.14.tar.bz2](http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.tar.bz2)

Currently we are not aware of any exploits for this vulnerability.

ID: 15156, October 31,  
2005

<p>Multiple Vendors</p> <p>zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3, 0.1-0.1.6 1, 0.0.1-0.0.6</p>	<p>A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code.</p> <p>Debian: <a href="ftp://security.debian.org/pool/updates/main/z/zlib/">ftp://security.debian.org/pool/updates/main/z/zlib/</a></p> <p>FreeBSD: <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch">ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch</a></p> <p>Gentoo: <a href="http://security.gentoo.org/glsa/glsa-200507-05.xml">http://security.gentoo.org/glsa/glsa-200507-05.xml</a></p> <p>SUSE: <a href="ftp://ftp.suse.com/pub/suse/">ftp://ftp.suse.com/pub/suse/</a></p> <p>Ubuntu: <a href="http://security.ubuntu.com/ubuntu/pool/main/z/zlib/">http://security.ubuntu.com/ubuntu/pool/main/z/zlib/</a></p> <p>Mandriva: <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p>OpenBSD: <a href="http://www.openbsd.org/errata.html">http://www.openbsd.org/errata.html</a></p> <p>OpenPKG: <a href="ftp.openpkg.org">ftp.openpkg.org</a></p> <p>RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-569.html">http://rhn.redhat.com/errata/RHSA-2005-569.html</a></p> <p>Trustix: <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p>Slackware: <a href="ftp://ftp.slackware.com/pub/slackware/">ftp://ftp.slackware.com/pub/slackware/</a></p> <p>TurboLinux: <a href="ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10">ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10</a></p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>zsync: <a href="http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download">http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download</a></p> <p>Apple: <a href="http://docs.info.apple.com/article.html?artnum=302163">http://docs.info.apple.com/article.html?artnum=302163</a></p> <p>SCO: <a href="ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33">ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33</a></p> <p>IPCop: <a href="http://sourceforge.net/project/showfiles.php?group_id=40604&amp;">http://sourceforge.net/project/showfiles.php?group_id=40604&amp;</a></p>	<p>Zlib Compression Library Buffer Overflow</p> <p><a href="#">CVE-2005-2096</a></p>	<p>High</p> <p>Debian Security Advisory DSA 740-1, July 6, 2005</p> <p>FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005</p> <p>Ubuntu Security Notice, USN-148-1, July 06, 2005</p> <p>RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0034, July 8, 2005</p> <p>Slackware Security Advisory, SSA:2005-189-01, July 11, 2005</p> <p>Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005</p> <p>Fedora Update Notification, FEDORA-2005-565, July 13, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005</p> <p>Security Focus, 14162, July 21, 2005</p> <p><a href="#">USCERT Vulnerability Note VU#680620, July 22, 2005</a></p> <p>Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005</p> <p>SCO Security Advisory, SCOSA-2005.33, August 19, 2005</p> <p>Security Focus, Bugtraq ID: 14162, August 26, 2005</p> <p>Debian Security Advisory, DSA 797-1, September 1,</p>
---	---	--	--



[package\\_id = 35093  
&release\\_id=351848](#)

Debian:  
<http://security.debian.org/pool/updates/main/z/zsync/>

Trolltech:  
<ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz>

FedoraLegacy:  
<http://download.fedoralegacy.org/fedora/>

Gentoo:  
<http://security.gentoo.org/glsa/glsa-200509-18.xml>

Gentoo:  
<http://security.gentoo.org/glsa/glsa-200509-18.xml>

Debian:  
<http://security.debian.org/pool/updates/main/z/zsync/>

Trustix:  
<http://http.trustix.org/pub/trustix/updates/>

Sun:  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101989-1>

**Mandriva:**  
<http://www.mandriva.com/security/advisories>

**Ubuntu:**  
<http://security.ubuntu.com/ubuntu/pool/main/a/aide/>

Currently we are not aware of any exploits for this vulnerability.

2005

Security Focus, Bugtraq  
ID: 14162, September 12, 2005

Fedora Legacy Update  
Advisory, FLSA:162680,  
September 14, 2005

Gentoo Linux Security  
Advisory, GLSA  
200509-18, September 26,  
2005

Debian Security Advisory,  
DSA 797-2, September  
29, 2005

Trustix Secure Linux  
Security Advisory,  
TSLSA-2005-0055,  
October 7, 2005

Sun(sm) Alert Notification  
Sun Alert ID: 101989,  
October 14, 2005

**Mandriva Linux Security  
Advisory  
MDKSA-2005:196,  
October 26, 2005**

**Ubuntu Security Notice,  
USN-151-3, October 28,  
2005**

<p>Multiple Vendors</p> <p>zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha</p>	<p>A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input.</p> <p>Zlib:  <a href="http://www.zlib.net/zlib-1.2.3.tar.gz">http://www.zlib.net/zlib-1.2.3.tar.gz</a></p> <p>Debian:  <a href="http://security.debian.org/pool/updates/main/z/zlib/">http://security.debian.org/pool/updates/main/z/zlib/</a></p> <p>Ubuntu:  <a href="http://security.ubuntu.com/ubuntu/pool/main/z/zlib/">http://security.ubuntu.com/ubuntu/pool/main/z/zlib/</a></p> <p>OpenBSD:  <a href="http://www.openbsd.org/errata.html#libz2">http://www.openbsd.org/errata.html#libz2</a></p> <p>Mandriva:  <a href="http://www.mandriva.com/security/advisories?name=MDKSA-2005:124">http://www.mandriva.com/security/advisories?name=MDKSA-2005:124</a></p> <p>Fedora:  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>Slackware:  <a href="http://slackware.com/security/viewer.php?l=slackware-security&amp;y=2005&amp;m=slackware-security.323596">http://slackware.com/security/viewer.php?l=slackware-security&amp;y=2005&amp;m=slackware-security.323596</a></p> <p>FreeBSD:  <a href="ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc">ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc</a></p> <p>SUSE:  <a href="http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html">http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html</a></p> <p>Gentoo:  <a href="http://security.gentoo.org/glsa/glsa-200507-28.xml">http://security.gentoo.org/glsa/glsa-200507-28.xml</a>  <a href="http://security.gentoo.org/glsa/glsa-200508-01.xml">http://security.gentoo.org/glsa/glsa-200508-01.xml</a></p> <p>Trustix:  <a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a></p> <p>Conectiva:  <a href="ftp://atualizacoes.conectiva.com.br/10/">ftp://atualizacoes.conectiva.com.br/10/</a></p> <p>Apple:  <a href="http://docs.info.apple.com/article.html?artnum=302163">http://docs.info.apple.com/article.html?artnum=302163</a></p> <p>TurboLinux:  <a href="ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/">ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/</a></p> <p>SCO:  <a href="ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33">ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33</a></p>	<p>Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service</p> <p><a href="#">CVE-2005-1849</a></p>	<p>Low</p> <p>Security Focus, Bugtraq ID 14340, July 21, 2005</p> <p>Debian Security Advisory DSA 763-1, July 21, 2005</p> <p>Ubuntu Security Notice, USN-151-1, July 21, 2005</p> <p>OpenBSD, Release Errata 3.7, July 21, 2005</p> <p>Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005</p> <p>Secunia, Advisory: SA16195, July 25, 2005</p> <p>Slackware Security Advisory, SSA:2005-203-03, July 22, 2005</p> <p>FreeBSD Security Advisory, SA-05:18, July 27, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0040, August 5, 2005</p> <p>Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005</p> <p>Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005</p> <p>Turbolinux Security Advisory, TLSA-2005-83, August 18, 2005</p> <p>SCO Security Advisory, SCOSA-2005.33, August 19, 2005</p> <p>Debian Security Advisory, DSA 797-1, September 1, 2005</p> <p>Security Focus, Bugtraq ID: 14340, September 12, 2005</p> <p>Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005</p> <p>Debian Security Advisory, DSA 797-2, September 29, 2005</p> <p><b>Mandriva Linux Security Advisory, MDKSA-2005:196, October 26, 2005</b></p> <p><b>Ubuntu Security Notice, USN-151-3, October 28, 2005</b></p>
---	--	---	---

Debian:  
<http://security.debian.org/pool/updates/main/z/zsync/>

Trolltech:  
<ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz>

FedoraLegacy:  
<http://download.fedoralegacy.org/fedora/>

Debian:  
<http://security.debian.org/pool/updates/main/z/zsync/>

**Mandriva:**  
<http://www.mandriva.com/security/advisories>

**Ubuntu:**  
<http://security.ubuntu.com/ubuntu/pool/main/a/aide/>

Currently we are not aware of any exploits for this vulnerability.

Multiple Vendors

Gentoo Linux;  
GNU GDB 6.3

Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when loading malformed object files, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported which could let a malicious user obtain elevated privileges.

Gentoo:  
<http://security.gentoo.org/glsa/glsa-200505-15.xml>

Ubuntu:  
<http://security.ubuntu.com/ubuntu/pool/main/g/gdb/>

<http://security.ubuntu.com/ubuntu/pool/main/b/binutils/>

Mandriva:  
<http://www.mandriva.com/security/advisories>

Trustix:  
<http://http.trustix.org/pub/trustix/updates/>

TurboLinux:  
<ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/>

RedHat:  
<http://rhn.redhat.com/errata/RHSA-2005-659.html>

RedHat:  
<http://rhn.redhat.com/errata/RHSA-2005-673.html>

<http://rhn.redhat.com/errata/RHSA-2005-709.html>

Avaya:  
<http://support.avaya.com/elmodocs2/security/ASA->

GDB Multiple Vulnerabilities

[CVE-2005-1704](#)  
[CVE-2005-1705](#)

High

Gentoo Linux Security Advisory, GLSA 200505-15, May 20, 2005

Turbolinux Security Advisory, TLSA-2005-68, June 22, 2005

RedHat Security Advisory, RHSA-2005:659-9, September 28, 2005

RedHat Security Advisory, RHSA-2005:673-5 & RHSA-2005:709-6, October 5, 2005

Avaya Security Advisory, ASA-2005-222, October 18, 2005

**Fedora Update Notifications, FEDORA-2005-1032 & 1033, October 27, 2005**

**Fedora:**

<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/>

Currently we are not aware of any exploits for these vulnerabilities.

<p>Multiple Vendors</p> <p>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</p>	<p>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.</p> <p>Debian: <a href="http://security.debian.org/pool/updates/main/libg/libgda2/">http://security.debian.org/pool/updates/main/libg/libgda2/</a></p> <p>Ubuntu: <a href="http://security.ubuntu.com/ubuntu/pool/main/libg/libgda2/">http://security.ubuntu.com/ubuntu/pool/main/libg/libgda2/</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>GNOME-DB LibGDA Multiple Format String</p> <p><a href="http://www.cve.org/CVE-2005-2958">CVE-2005-2958</a></p>	<p>High</p>	<p>Security Focus, Bugtraq ID: 15200, October 25, 2005</p> <p>Debian Security Advisory, DSA-871-1 &amp; 871-2, October 25, 2005</p> <p><b>Ubuntu Security Notice, USN-212-1, October 28, 2005</b></p>
<p>Multiple Vendors</p> <p>GNU gnump3d 2.9-2.9.5; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha</p>	<p>A vulnerability has been reported in GNUMP3d that could let remote malicious users conduct Cross-Site Scripting or traverse directories.</p> <p>Upgrade to version 2.9.6: <a href="http://savannah.gnu.org/download/gnump3d/gnump3d-2.9.6.tar.gz">http://savannah.gnu.org/download/gnump3d/gnump3d-2.9.6.tar.gz</a></p> <p>Debian: <a href="http://security.debian.org/pool/updates/main/g/gnump3d/">http://security.debian.org/pool/updates/main/g/gnump3d/</a></p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>GNUMP3d Cross-Site Scripting or Directory Traversal</p> <p><a href="http://www.cve.org/CVE-2005-3122">CVE-2005-3122</a> <a href="http://www.cve.org/CVE-2005-3123">CVE-2005-3123</a></p>	<p>Medium</p>	<p>Security Focus Bugtraq IDs: 15226 &amp; 15228, October 28, 2005</p> <p>Debian Security Advisory DSA 877-1, October 28, 2005</p>
<p>Multiple Vendors</p> <p>Linux kernel 2.6-2.6.14</p>	<p>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 with zeroes when increasing the length, which could let a malicious user obtain sensitive information.</p> <p>Patches available at: <a href="http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.14-rc4.bz2">http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.14-rc4.bz2</a></p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>Trustix: <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p>RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-808.html">http://rhn.redhat.com/errata/RHSA-2005-808.html</a></p> <p>There is no exploit code required.</p>	<p>Linux Kernel Denial of Service &amp; Information Disclosure</p> <p><a href="http://www.cve.org/CVE-2005-3119">CVE-2005-3119</a> <a href="http://www.cve.org/CVE-2005-3180">CVE-2005-3180</a> <a href="http://www.cve.org/CVE-2005-3181">CVE-2005-3181</a></p>	<p>Medium</p>	<p>Secunia Advisory: SA17114, October 12, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0057, October 14, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-1013, October 20, 2005</p> <p><b>RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005</b></p>
<p>Multiple Vendors</p> <p>Linux Kernel 2.6-2.6.14</p>	<p>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</p>	<p>Multiple Vendors Linux Kernel Denials of Service</p>	<p>Low</p>	<p>Ubuntu Security Notice, USN-199-1, October 10, 2005</p> <p>Trustix Secure Linux</p>

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 a 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/>

RedHat:  
<http://rhn.redhat.com/errata/RHSA-2005-808.html>

Currently we are not aware of any exploits for these vulnerabilities.

[CVE-2005-3053](#)  
[CVE-2005-3106](#)  
[CVE-2005-3107](#)  
[CVE-2005-3108](#)  
[CVE-2005-3109](#)  
[CVE-2005-3110](#)

Security Advisory, TSLSA-2005-0057, October 14, 2005

**RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005**

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/>

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,

	<p>OpenPKG: <a href="http://ftp.openpkg.org/release/">ftp://ftp.openpkg.org/release/</a></p> <p>SUSE: <a href="http://ftp.SUSE.com/pub/SUSE">ftp://ftp.SUSE.com/pub/SUSE</a></p> <p>Trustix: <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p>SGL: <a href="http://www.sgi.com/support/security/">http://www.sgi.com/support/security/</a></p> <p><b>Debian:</b> <a href="http://security.debian.org/pool/updates/main/o/openssl094/">http://security.debian.org/pool/updates/main/o/openssl094/</a></p> <p><b>NetBSD:</b> <a href="http://arkiv.netbsd.se/?ml=netbsd-announce&amp;a=2005-10&amp;m=1435804">http://arkiv.netbsd.se/?ml=netbsd-announce&amp;a=2005-10&amp;m=1435804</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>		<p>October 21, 2005</p> <p>SGI Security Advisory, 20051003-01-U, October 26, 2005</p> <p><b>Debian Security Advisory DSA 875-1, October 27, 2005</b></p> <p><b>NetBSD Security Update, November 1, 2005</b></p>
<p>Multiple Vendors</p> <p>RedHat Fedora Core4, Core3, RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Linux-PAM Linux-PAM 0.77; Gentoo Linux</p>	<p>A vulnerability has been reported in Pluggable Authentication Modules that could let local malicious users to bypass security restrictions.</p> <p>Redhat: <a href="https://rhn.redhat.com/errata/RHSA-2005-805.html">https://rhn.redhat.com/errata/RHSA-2005-805.html</a></p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>Gentoo: <a href="http://security.gentoo.org/glsa/glsa-200510-22.xml">http://security.gentoo.org/glsa/glsa-200510-22.xml</a></p> <p>There is no exploit code required.</p>	<p>Pluggable Authentication Modules Security Bypassing</p> <p><a href="#">CVE-2005-2977</a></p>	<p>Medium</p> <p>RedHat Security Advisory, RHSA-2005:805-6, October 26, 2005</p> <p>Fedora Update Notifications FEDORA-2005-1030 &amp; 1031, October 27, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200510-22, October 28, 2005</p>
<p>Multiple Vendors</p> <p>Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Netpbm 10.0</p>	<p>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.</p> <p>Ubuntu: <a href="http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/">http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/</a></p> <p>RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-793.html">http://rhn.redhat.com/errata/RHSA-2005-793.html</a></p> <p>Gentoo: <a href="http://security.gentoo.org/glsa/glsa-200510-18.xml">http://security.gentoo.org/glsa/glsa-200510-18.xml</a></p> <p>SUSE: <a href="ftp://ftp.SUSE.com/pub/SUSE">ftp://ftp.SUSE.com/pub/SUSE</a></p> <p>Mandriva: <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p><b>Debian:</b> <a href="http://security.debian.org/pool/updates/">http://security.debian.org/pool/updates/</a></p>	<p>NetPBM Buffer Overflow</p> <p><a href="#">CVE-2005-2978</a></p>	<p>High</p> <p>Ubuntu Security Notice, USN-210-1, October 18, 2005</p> <p>RedHat Security Advisory, RHSA-2005:793-6, October 18, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200510-18, October 20, 2005</p> <p>SUSE Security Summary Report, Announcement ID: SUSE-SR:2005:024, October 21, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2005:199, October 26, 2005</p> <p><b>Debian Security Advisory, DSA 878-1, October 28, 2005</b></p>

[main/n/netpbm-free/](#)

Currently we are not aware of any exploits for this vulnerability.

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.

**NetBSD:**  
<http://arkiv.netbsd.se/?ml=netbsd-announce&a=2005-10&m=1435804>

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, TLSA-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

**NetBSD Security Update, October 31, 2005**

<p>OpenVPN</p> <p>OpenVPN 2.0-2.0.2</p>	<p>Several vulnerabilities have been reported: a format string vulnerability was reported in 'options.c' when handling command options in the 'foreign_option()' function, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported due to a NULL pointer dereferencing error in the OpenVPN server when running in TCP mode.</p> <p>Updates available at:  <a href="http://openvpn.net/download.html">http://openvpn.net/download.html</a></p> <p>OpenPKG:  <a href="ftp://ftp.openpkg.org/release/">ftp://ftp.openpkg.org/release/</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>OpenVPN Client Remote Format String &amp; Denial of Service</p> <p><a href="http://cve.mitre.org/cgi-bin/cveghana/show.cgi?ID=CVE-2005-3393">CVE-2005-3393</a></p>	<p>High</p>	<p>Secunia Advisory: SA17376, November 1, 2005</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2005.023, November 2, 2005</p>
<p>SCO</p> <p>UnixWare Portmapper</p>	<p>A vulnerability has been reported in UnixWare Portmapper that could let remote malicious users cause a Denial of Service.</p> <p><b>SCO:</b>  <a href="ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.43">ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.43</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>UnixWare Portmapper Denial of Service</p> <p><a href="http://cve.mitre.org/cgi-bin/cveghana/show.cgi?ID=CVE-2005-2132">CVE-2005-2132</a></p>	<p>Low</p>	<p>Security Focus, 14360, July 25, 2005</p> <p><b>SCO Security Advisory, SCOSA-2005.43, October 27, 2005</b></p>
<p>Sun Microsystems, Inc.</p> <p>Sun Solaris 8, 9, 10</p>	<p>A vulnerability has been reported in Sun Solaris, Solaris Management Console, that could let local malicious users conduct Cross-Site Scripting.</p> <p>Vendor solution available:  <a href="http://sunsolve.sun.com/search/document.do?assetkey=1-26-102016-1">http://sunsolve.sun.com/search/document.do?assetkey=1-26-102016-1</a></p> <p>There is no exploit code required.</p>	<p>Sun Solaris Cross-Site Scripting</p> <p><a href="http://cve.mitre.org/cgi-bin/cveghana/show.cgi?ID=CVE-2005-3398">CVE-2005-3398</a></p>	<p>Medium</p>	<p>Sun, Alert ID: 102016, October 26, 2005</p>
<p>Sun Microsystems, Inc.</p> <p>Sun Java System Communications Express</p>	<p>A vulnerability has been reported due to an unspecified error that can be exploited by local/remote malicious users to obtain sensitive information.</p> <p>Patches available at:  <a href="http://sunsolve.sun.com/search/document.do?assetkey=1-26-101948-1">http://sunsolve.sun.com/search/document.do?assetkey=1-26-101948-1</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Sun Java System Communications Express Information Disclosure</p> <p><a href="http://cve.mitre.org/cgi-bin/cveghana/show.cgi?ID=CVE-2005-3472">CVE-2005-3472</a></p>	<p>Medium</p>	<p>Sun(sm) Alert Notification Sun Alert ID: 101948, November 1, 2005</p>
<p>Sun Micro-systems, Inc.</p> <p>Solaris 10.0, 9.0_x86, 9.0</p>	<p>A vulnerability has been reported in LD_AUDIT,' which could let a malicious user obtain superuser privileges.</p> <p>Workaround and patch information available at:  <a href="http://sunsolve.sun.com/search/document.do?assetkey=1-26-101794-1">http://sunsolve.sun.com/search/document.do?assetkey=1-26-101794-1</a></p> <p>Avaya:  <a href="http://support.avaya.com/elmodocs2/security/ASA-2005-162.pdf">http://support.avaya.com/elmodocs2/security/ASA-2005-162.pdf</a></p> <p>An exploit script has been published.</p>	<p>Sun Solaris Runtime Linker 'LD_AUDIT' Elevated Privileges</p> <p><a href="http://cve.mitre.org/cgi-bin/cveghana/show.cgi?ID=CVE-2005-2072">CVE-2005-2072</a></p>	<p>High</p>	<p>Security Focus, 14074, June 28, 2005</p> <p>Sun(sm) Alert Notification, 101794, June 28, 2005</p> <p>Sun(sm) Alert Notification, 101794, Updated July 12, 13, 15, 2005</p> <p>Avaya Security Advisory, ASA-2005-162, August 2, 2005</p> <p><b>Sun(sm) Alert Notification, 101794, Updated October 31, 2005</b></p>



<p>Todd Miller</p> <p>Sudo 1.x</p>	<p>A vulnerability has been reported in the environment cleaning due to insufficient sanitization, which could let a malicious user obtain elevated privileges.</p> <p>Debian: <a href="http://security.debian.org/pool/updates/main/s/sudo/">http://security.debian.org/pool/updates/main/s/sudo/</a></p> <p><b>Mandriva:</b> <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p><b>Ubuntu:</b> <a href="http://security.ubuntu.com/ubuntu/pool/main/s/sudo/">http://security.ubuntu.com/ubuntu/pool/main/s/sudo/</a></p> <p>There is no exploit code required.</p>	<p>Todd Miller Sudo Local Elevated Privileges</p> <p><a href="#">CVE-2005-2959</a></p>	<p>Medium</p>	<p>Debian Security Advisory, DSA 870-1, October 25, 2005</p> <p><b>Mandriva Linux Security Advisory, MDKSA-2005:201, October 27, 2005</b></p> <p><b>Ubuntu Security Notice, USN-213-1, October 28, 2005</b></p>
<p>Uim</p> <p>Uim 0.5 .0, 0.4.9</p>	<p>A vulnerability has been reported in 'uim/uim-custom.c' due to the incorrect use of several environment variables, which could let a malicious user obtain elevated privileges.</p> <p>Updates available at: <a href="http://uim.freedesktop.org/releases/uim-0.4.9.1.tar.gz">http://uim.freedesktop.org/releases/uim-0.4.9.1.tar.gz</a></p> <p><b>Mandriva:</b> <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p>There is no exploit code required.</p>	<p>Uim Elevated Privileges</p> <p><a href="#">CVE-2005-3149</a></p>	<p>Medium</p>	<p>Secunia Advisory: SA17043, October 4, 2005</p> <p><b>Mandriva Linux Security Update Advisory, MDKSA-2005:198, October 26, 2005</b></p>
<p>xloadimage</p> <p>xloadimage 4.1</p>	<p>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.</p> <p>Debian: <a href="http://security.debian.org/pool/updates/main/x/xloadimage/">http://security.debian.org/pool/updates/main/x/xloadimage/</a> <a href="http://security.debian.org/pool/updates/main/x/xli/">http://security.debian.org/pool/updates/main/x/xli/</a></p> <p>RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-802.html">http://rhn.redhat.com/errata/RHSA-2005-802.html</a></p> <p><b>Mandriva:</b> <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p>SUSE: <a href="ftp://ftp.SUSE.com/pub/SUSE">ftp://ftp.SUSE.com/pub/SUSE</a></p> <p>SGL: <a href="http://www.sgi.com/support/security/">http://www.sgi.com/support/security/</a></p> <p><b>Gentoo:</b> <a href="http://security.gentoo.org">http://security.gentoo.org</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Xloadimage NIFF Image Buffer Overflow</p> <p><a href="#">CVE-2005-3178</a></p>	<p><b>High</b></p>	<p>Debian Security Advisories, DSA 858-1 &amp; 859-1, October 10, 2005</p> <p>RedHat Security Advisory, RHSA-2005:802-4, October 18, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:191, October 21, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:024, October 21, 2005</p> <p>SGI Security Advisory, 20051003-01-U, October 26, 2005</p> <p><b>Gentoo Linux Security Advisory, GLSA 200510-26, October 31, 2005</b></p>

[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

<p>Alexander Palmo</p> <p>Simple PHP Blog 0.4.5 &amp; prior</p>	<p>Cross-Site Scripting vulnerabilities have been reported in 'preview_cgi.php' and 'preview_static_cgi.php' due to insufficient sanitization of the 'entry' parameter, in 'preview_cgi.php' due to insufficient sanitization of the 'blog_subject' and 'blog_text' parameters, in 'preview_static_cgi.php' due to insufficient sanitization of the 'blog_subject,' 'blog_text,' and 'file_name' parameters, and in 'colors_cgi.php' due to insufficient sanitization of the 'scheme_name' and the 'bg_color' parameters, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>Simple PHP Blog Cross-Site Scripting</p> <p><a href="#">CVE-2005-3473</a></p>	<p>Medium</p>	<p>Technical University of Vienna Security Advisory TUVSA-0511-001, November 2, 2005</p>
<p>ATutor</p> <p>ATutor 1.5.1-pl1, 1.5.1, 1.4.1-1.4.3</p> <p>ATutor</p>	<p>Multiple vulnerabilities have been reported in ATutor that could let remote malicious users conduct Cross-Site Scripting, disclose sensitive information, or execute arbitrary code.</p> <p>Vendor patch available: <a href="http://atutor.ca/view/3/6158/1.html">http://atutor.ca/view/3/6158/1.html</a></p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>ATutor Multiple Vulnerabilities</p> <p><a href="#">CVE-2005-3403</a> <a href="#">CVE-2005-3404</a> <a href="#">CVE-2005-3405</a></p>	<p>High</p>	<p>Secunia, Advisory: SA16915, October 27, 2005</p>
<p>Cisco Systems</p> <p>CiscoWorks Management Center for IPS Sensors (IPSMC) 2.1</p>	<p>A vulnerability has been reported due to an error in the Cisco IOS IPS (Intrusion Prevention System) configuration file that is generated by the IPS MC and deployed to IOS IPS devices, which could potentially allow malicious traffic to pass through.</p> <p>Patch information available at: <a href="http://www.cisco.com/warp/public/707/cisco-sa-20051101-ipsmc.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20051101-ipsmc.shtml</a></p> <p>There is no exploit code required.</p>	<p>Cisco Management Center for IPS Sensors Signature Disable</p> <p><a href="#">CVE-2005-3427</a></p>	<p>Medium</p>	<p>Cisco Security Advisory, 68065, November 1, 2005</p> <p><a href="#">US-CERT VU#154883</a></p>
<p>codetosell.com</p> <p>ViArt Shop Enterprise 2.x</p>	<p>Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'basket.php,' 'forum.php,' 'page.php,' 'reviews.php,' 'products.php,' and 'news_view.php' scripts due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability was reported in the 'forum_new_thread.php' script due to insufficient sanitization of input passed to the nickname, email, topic and message fields and the nickname and message fields in 'forum_threads.php,' which could let a remote malicious user execute arbitrary HTML and script code.</p> <p><b>ViArt Shop Enterprise 2.1.8 &amp; prior versions are not affected by these issues. Please contact the vendor to obtain a fixed version.</b></p> <p>There is no exploit code required; however, Proofs of Concepts have been published.</p>	<p>ViArt Shop Enterprise Cross-Site Scripting</p> <p><a href="#">CVE-2005-1440</a></p>	<p>High</p>	<p>Secunia Advisory, SA15181, May 2, 2005</p> <p><b>Security Focus, Bugtraq ID: 13462, October 27, 2005</b></p>
<p>eyeOS</p> <p>eyeOS 0.8.4 -r1, 0.8.4, 0.8.3 -r2, 0.8.3</p>	<p>Several vulnerabilities have been reported: a vulnerability was reported in 'desktop.php' due to insufficient sanitization of the 'motd' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because user credentials are stored in the file 'usrinfo.xml' inside the web root, which could let a remote malicious user obtain sensitive information.</p> <p>Update available at: <a href="http://www.eyeos.org/?section=Downloads">http://www.eyeos.org/?section=Downloads</a></p> <p>There is no exploit code required.</p>	<p>eyeOS Script Insertion &amp; Information Disclosure</p> <p><a href="#">CVE-2005-3413</a> <a href="#">CVE-2005-3414</a></p>	<p>Medium</p>	<p>Secunia Advisory: SA17105, November 1, 2005</p>
<p>First4Internet Ltd.</p> <p>XCP Content Management</p>	<p>A vulnerability has been reported in 'aries.sys' due to the device driver hiding all files, registry keys and processes on the system that have names that start with "\$sys\$", which could let a malicious user bypass security.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>First4Internet XCP Content Management Security Bypass</p> <p><a href="#">CVE-2005-3474</a></p>	<p>Medium</p>	<p>Secunia Advisory: SA17408, November 2, 2005</p>

gCards gCards 1.44	An SQL injection vulnerability has been reported in 'news.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 has been published.	gCards SQL Injection  <a href="#">CVE-2005-3408</a>	Medium	Security Tracker, Alert ID: 1015106, October 25, 2005
Hasbani Hasbani Web Server	A vulnerability has been reported in Hasbani Web Server that could let remote malicious users cause a Denial of Service.  No workaround or patch available at time of publishing.  An exploit has been published.	Hasbani Web Server Denial of Service  <a href="#">CVE-2005-3475</a>	Low	Security Focus, ID: 15225, October 27, 2005
Hewlett Packard Company OpenVMS Integrity 8.2-1, 8.2, OpenVMS Alpha 7.3-2, 8.2	A Denial of Service vulnerability has been reported due to an unspecified error.  Patch available at: <a href="http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBOV01239">http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBOV01239</a>  Currently we are not aware of any exploits for this vulnerability.	HP OpenVMS Denial of Service  <a href="#">CVE-2005-3476</a>	Low	HP Security Bulletin, HPSBOV01239, October 31, 2005
Invision Power Services Invision Gallery 2.0.3	A vulnerability has been reported in the image 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.	Invision Gallery Image Input Validation  <a href="#">CVE-2005-3477</a>	Medium	Secunia Advisory: SA17393, November 2, 2005
Invision Power Services Invision Gallery 2.0.3	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the the 'st' 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.	Invision Gallery SQL Injection  <a href="#">CVE-2005-3395</a>	Medium	Secunia Advisory: SA17375, November 1, 2005
Jed Wing CHM lib 0.35, 0.3- 0.33, 0.2, 0.1	A buffer overflow vulnerability has been reported in '_chm_find_in_PMG'L' due to a failure to properly bounds check input data prior to copying it into an insufficiently sized memory buffer, which could let a remote malicious user execute arbitrary code.  Upgrades available at: <a href="http://morte.jedrea.com/~jedwin/projects/chmlib/chmlib-0.36.tgz">http://morte.jedrea.com/~jedwin/projects/chmlib/chmlib-0.36.tgz</a>  Currently we are not aware of any exploits for this vulnerability.	Jed Wing CHM Lib '_chm_find_in_PMG'L Remote Buffer Overflow  <a href="#">CVE-2005-2930</a>	High	iDefense Security Advisory, October 28, 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 the User ID is cached longer than necessary.  Upgrades available at: <a href="http://prdownloads.sourceforge.net/mantisbt/mantis-0.19.3.tar.gz">http://prdownloads.sourceforge.net/mantisbt/mantis-0.19.3.tar.gz</a>  <b>Gentoo:</b> <a href="http://security.gentoo.org/glsa/glsa-200510-24.xml">http://security.gentoo.org/glsa/glsa-200510-24.xml</a>  There is no exploit code required; however, Proof of Concept exploits have been published.	Mantis Multiple Vulnerabilities  <a href="#">CVE-2005-3335</a> <a href="#">CVE-2005-3336</a> <a href="#">CVE-2005-3337</a> <a href="#">CVE-2005-3338</a> <a href="#">CVE-2005-3339</a>	High	Secunia Advisory: SA16818, October 26, 2005  <b>Gentoo Linux Security Advisory, GLSA 200510-24, October 28, 2005</b>

<p>Multiple Vendors</p> <p>ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10- PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLE pre122300, -STABLE pre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 - STABLE, -RELENG, 4.3 -RELEASE -p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLE pre2002- 03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE -p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRE RELEASE, 4.8, 4.9 -RELENG, 4.9 -PRE RELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRE RELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386; SGI IRIX 6.5.24-6.5.27</p>	<p>Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()'  function, which could let a remote malicious user execute arbitrary code.</p> <p>ALTLinux: <a href="http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html">http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html</a></p> <p>Apple: <a href="http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05529&amp;platform=osx&amp;method=sa/SecUpd%202005-003Pan.dmg">http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05529&amp;platform=osx&amp;method=sa/SecUpd 2005-003Pan.dmg</a></p> <p>Debian: <a href="http://security.debian.org/pool/updates/main/n/netkit-telnet/">http://security.debian.org/pool/updates/main/n/netkit-telnet/</a></p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>FreeBSD: <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/">ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/</a></p> <p>MIT Kerberos: <a href="http://web.mit.edu/kerberos/advisories/2005-001-patch_1.4.txt">http://web.mit.edu/kerberos/advisories/2005-001-patch_1.4.txt</a></p> <p>Netkit: <a href="ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/">ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/</a></p> <p>Openwall: <a href="http://www.openwall.com/Owl/CHANGES-current.shtml">http://www.openwall.com/Owl/CHANGES-current.shtml</a></p> <p>RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-327.html">http://rhn.redhat.com/errata/RHSA-2005-327.html</a></p> <p>Sun: <a href="http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1">http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1</a></p> <p>SUSE: <a href="ftp://ftp.SUSE.com/pub/SUSE">ftp://ftp.SUSE.com/pub/SUSE</a></p> <p>Ubuntu: <a href="http://security.ubuntu.com/ubuntu/pool/main/n/netkit-telnet/">http://security.ubuntu.com/ubuntu/pool/main/n/netkit-telnet/</a></p> <p>OpenBSD: <a href="http://www.openbsd.org/errata.html#telnet">http://www.openbsd.org/errata.html#telnet</a></p> <p>Mandrake: <a href="http://www.mandrakesecure.net/en/ftp.php">http://www.mandrakesecure.net/en/ftp.php</a></p> <p>Gentoo: <a href="http://security.gentoo.org/glsa/glsa-200503-36.xml">http://security.gentoo.org/glsa/glsa-200503-36.xml</a>  <a href="http://security.gentoo.org/glsa/glsa-200504-01.xml">http://security.gentoo.org/glsa/glsa-200504-01.xml</a></p> <p>Debian:</p>	<p>Telnet Client 'slc_add_reply()' &amp; 'env_opt_add()' Buffer Overflows  <a href="http://cve.mitre.org/cve/2005/0468">CVE-2005-0468</a> <a href="http://cve.mitre.org/cve/2005/0469">CVE-2005-0469</a></p>	<p>High</p> <p>DEFENSE Security Advisory, March 28, 2005 <a href="http://www.cisa.gov/uscert/psa/secalert/vu050336a.html">US-CERT VU#291924</a></p> <p>Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005</p> <p>Gentoo Linux Security Advisories, GLSA 200503-36 &amp; GLSA 200504-01, March 31 &amp; April 1, 2005</p> <p>Debian Security Advisory, DSA 703-1, April 1, 2005 <a href="http://www.debian.org/security/2005/dsa7031.html">US-CERT VU#341908</a></p> <p>Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005</p> <p>SGI Security Advisory, 20050401-01-U, April 6, 2005</p> <p>Sun(sm) Alert Notification, 57761, April 7, 2005</p> <p>SCO Security Advisory, SCOSA-2005.21, April 8, 2005</p> <p>Avaya Security Advisory, ASA-2005-088, April 27, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200504-28, April 28, 2005</p> <p>Turbolinux Security Advisory, TLSA-2005-52, April 28, 2005</p> <p>Sun(sm) Alert Notification, 57761, April 29, 2005</p> <p>SCO Security Advisory, SCOSA-2005.23, May 17, 2005</p> <p>SGI Security Advisory, 20050405-01-P, May 26, 2005</p> <p>Debian Security Advisory, DSA 731-1, June 2, 2005</p> <p>Conectiva Security Advisory, CLSA-2005:962, June 6, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005</p> <p>Avaya Security Advisory,</p>
--	--	--	--

<http://security.debian.org/pool/updates/main/k/krb5/>

Gentoo:  
<http://security.gentoo.org/glsa/glsa-200504-04.xml>

SGI:  
[ftp://oss.sgi.com/projects/sji\\_propack/download/3/updates/](ftp://oss.sgi.com/projects/sji_propack/download/3/updates/)

SCO:  
<ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.21>

Sun:  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1>

Openwall:  
<http://www.openwall.com/Owl/CHANGES-current.shtml>

Avaya:  
<http://support.avaya.com/elmodocs2/security/ASA-2005-088>  
[RHSA-2005-330.pdf](#)

Gentoo:  
<http://security.gentoo.org/glsa/glsa-200504-28.xml>

TurboLinux:  
<ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/>

Sun:  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1>

OpenWall:  
<http://www.openwall.com/Owl/CHANGES-current.shtml>

SCO:  
<ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.23>

SGI IRIX:  
Apply patch 5892 for IRIX 6.5.24-6.5.27:  
<ftp://patches.sgi.com/support/free/security/patches/>

Debian:  
<http://security.debian.org/pool/updates/main/k/krb4/>

Conectiva:  
<http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000962>

Trustix:  
<ftp://ftp.trustix.org/pub/trustix/updates/>

Avaya:  
<http://support.avaya.com/elmodocs2/security/ASA-2005-132>  
[RHSA-2005-327.pdf](#)

FedoraLegacy:  
<http://download.fedoralegacy>

ASA-2005-132, June 14, 2005

Fedora Legacy Update Advisory, FLSA:152583, July 11, 2005

Slackware Security Advisory, SSA:2005-210-01, August 1, 2005

Debian Security Advisory, DSA 773-1, August 11, 2005

**Security Focus, Bugtraq ID: 12919, November 1, 2005**

[org/redhat/](#)

Slackware:  
<ftp://ftp.slackware.com/pub/slackware/>

Debian:  
<http://security.debian.org/pool/updates/main/>

**NetBSD 2.0.3 is not vulnerable to this issue. Please contact the vendor for more information.**

Currently we are not aware of any exploits for these vulnerabilities.

Multiple Vendors

Concurrent Versions System (CVS) 1.x; Gentoo Linux; SuSE Linux 8.2, 9.0, 9.1, x86\_64, 9.2, x86\_64, 9.3, Linux Enterprise Server 9, 8, Open-Enterprise-Server 9.0, School-Server 1.0, SUSE CORE 9 for x86, UnitedLinux 1.0

Update available at:  
<https://ccvs.cvshome.org/servlets/ProjectDocumentList>

Gentoo:  
<http://security.gentoo.org/glsa/glsa-200504-16.xml>

SuSE:  
<ftp://ftp.suse.com/pub/suse/>

Fedora:  
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>

Mandrake:  
<http://www.mandrakesecure.net/en/ftp.php>

Trustix:  
<http://http.trustix.org/pub/trustix/updates/>

FreeBSD:  
<ftp://ftp.FreeBSD.org/pub/>

Peachtree:  
<http://peachtree.burdell.org/updates/>

RedHat:  
<http://rhn.redhat.com/errata/RHSA-2005-387.html>

OpenBSD:  
<http://www.openbsd.org/errata.html#cv>

TurboLinux:  
<ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/>

OpenBSD:  
<http://www.openbsd.org/errata35.html#>

Ubuntu:  
<http://security.ubuntu.com/Subunit/pool/main/c/cvs/>

SGI:  
<ftp://patches.sgi.com/support/free/security/advisories/>

OpenBSD:

CVS Multiple Vulnerabilities  
[CVE-2005-0753](#)

High

Gentoo Linux Security Advisory, GLSA 200504-16, April 18, 2005

SuSE Security Announcement, SUSE-SA:2005:024, April 18, 2005

Secunia Advisory, SA14976, April 19, 2005

Fedora Update Notification, FEDORA-2005-330, April 20, 2006

Mandriva Linux Security Update Advisory, MDKSA-2005:073, April 21, 2005

Trustix Secure Linux Security Advisory, TSLSA-2005-0013, April 21, 2005

Gentoo Linux Security Advisory [UPDATE], GLSA 200504-16:02, April 22, 2005

FreeBSD Security Advisory, FreeBSD-SA-05:05, April 22, 2005

Peachtree Linux Security Notice, PLSN-0005, April 22, 2005

RedHat Security Advisory, RHSA-2005:387-06, April 25, 2005

Turbolinux Security Advisory, TSLA-2005-51, April 28, 2005

Ubuntu Security Notice, USN-117-1, May 04, 2005

SGI Security Advisory, 20050501-01-U, May 5, 2005

Conectiva Security Advisory, CLSA-2005:966, June 13, 2005

Debian Security Advisory, DSA 773-1, August 11, 2005

<http://www.openbsd.org/errata.html#cvs>

Conectiva:

<http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000966>

Debian:

<http://security.debian.org/pool/updates/main>

**NetBSD:**

<http://www.NetBSD.org/>

Currently we are not aware of any exploits for these vulnerabilities.

**NetBSD Security Update, November 1, 2005**

Multiple Vendors

MandrakeSoft Linux  
Mandrake 2006.0 x86\_64, 2006.0, 10.2 x86\_64, 10.2;  
Gentoo Linux;  
Ethereal Group Ethereal  
0.10.1-0.10.13, 0.9-0.9.16,  
0.8.19, 0.8.18, 0.8.13-0.8.15,  
0.8.5, 0.8, 0.7.7

A vulnerability has been reported in Ethereal, IRC Protocol Dissector, that could let remote malicious users cause a Denial of Service.

Mandriva:

<http://www.mandriva.com/security/advisories>

Gentoo:

<http://security.gentoo.org/glsa/glsa-200510-25.xml>

Currently we are not aware of any exploits for this vulnerability.

Ethereal Denial of Service

[CVE-2005-3313](#)

Low

Mandriva Linux Security Advisory, MDKSA-2005:193-1, October 26, 2005

Gentoo Linux Security Advisor, GLSA 200510-25, October 30, 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 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>

**Avaya:**

<http://support.avaya.com/elmodocs2/security/ASA-2005-227.pdf>

**Gentoo:**

<http://security.gentoo.org/glsa/glsa-200510-25.xml>

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

**Avaya Security Advisory, ASA-2005-227, October 28, 2005**

**Gentoo Linux Security Advisory, GLSA 200510-25, October 30, 2005**

**Mandriva Linux Security Advisory, MDKSA-2005:193-2, October 31, 2005**

An exploit script has been published.

Multiple Vendors  
Ukrainian 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.  
**Trend Micro PC-cillin 2006 is not affected by this issue. Please contact the vendor to obtain fixes.**  
A Proof of Concept exploit has been published.

Multiple Vendors  
Anti-Virus Magic Byte Detection Evasion  
[CVE-2005-3370](#)  
[CVE-2005-3371](#)  
[CVE-2005-3372](#)  
[CVE-2005-3373](#)  
[CVE-2005-3374](#)  
[CVE-2005-3375](#)  
[CVE-2005-3376](#)  
[CVE-2005-3377](#)  
[CVE-2005-3378](#)  
[CVE-2005-3379](#)  
[CVE-2005-3380](#)  
[CVE-2005-3381](#)  
[CVE-2005-3382](#)  
[CVE-2005-3399](#)  
[CVE-2005-3400](#)  
[CVE-2005-3401](#)

High

Security Focus,  
Bugtraq ID: 15189,  
October 25, 2005  
**Security Focus,  
Bugtraq ID: 15189,  
October 31, 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:  
<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/>  
Ubuntu:  
<http://security.ubuntu.com/ubuntu/pool/main/l/lynx/>

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  
Mandriva Linux Security Advisory, MDKSA-2005:186-1, October 26, 2005  
Debian Security Advisories, DSA 874-1 & 876-1, October 27, 2005  
**Ubuntu Security Notice, USN-206-2, October 29, 2005**



(Note: Ubuntu advisory USN-206-1 was previously released to address this vulnerability, however, the fixes contained an error that caused lynx to crash.)

A Proof of Concept Denial of Service exploit script has been published.

<p>Novell ZENworks Patch Management 6.0.0.52</p>	<p>A vulnerability has been reported in ZENworks Patch Management that could let local malicious users perform SQL injection.</p> <p>Upgrade to version 6.2.2.181: <a href="http://download.novell.com">http://download.novell.com</a></p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>Novell ZENworks Patch Management SQL Injection <a href="#">CVE-2005-3315</a></p>	<p>Medium</p>	<p>Novell, TID1009318, October 27, 2005</p>
<p>OaBoard OaBoard 1.0</p>	<p>An SQL injection vulnerability has been reported in 'forum.php' due to insufficient sanitization of the 'channel' and 'topic' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>OaBoard SQL Injection <a href="#">CVE-2005-3394</a></p>	<p>Medium</p>	<p>Secunia Advisory: SA17373, November 1, 2005</p>
<p>PBLang PBLang 4.65</p>	<p>Multiple vulnerabilities have been reported in PBLang that could let remote malicious users conduct Cross-Site Scripting or execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>PBLang Multiple Cross-Site Scripting Vulnerabilities</p>	<p>High</p>	<p>Security Focus, ID: 15223, October 27, 2005</p>
<p>PHP Advanced Transfer Manager PHP Advanced Transfer Manager 1.30</p>	<p>A vulnerability has been reported in PHP Advanced Transfer Manager that could let remote malicious users obtain unauthorized access.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>PHP Advanced Transfer Manager Unauthorized Access</p>	<p>Medium</p>	<p>Security Focus, ID: 15237, October 29, 2005</p>
<p>PHP Group PHP 5.0.5, 4.4.0</p>	<p>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.</p> <p>Ubuntu: <a href="http://security.ubuntu.com/ubuntu/pool/main/p/php4/">http://security.ubuntu.com/ubuntu/pool/main/p/php4/</a></p> <p>Trustix: <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p><b>Upgrades available at:</b> <a href="http://www.php.net/">http://www.php.net/</a></p> <p>There is no exploit code required.</p>	<p>PHP 'Open_BaseDir' Information Disclosure <a href="#">CVE-2005-3054</a></p>	<p>Medium</p>	<p>Security Focus, Bugtraq ID: 14957, September 27, 2005</p> <p>Ubuntu Security Notice, USN-207-1, October 17, 2005</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005</p> <p><b>Security Focus, Bugtraq ID: 14957, October 31, 2005</b></p>
<p>PHP PHP 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x, 5.0.x</p>	<p>Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of the 'GLOBALS' array, which could let a remote malicious user define global variables; a vulnerability was reported in the 'parse_str()' PHP function when handling an unexpected termination, which could let a remote malicious user enable the 'register_globals' directive; a Cross-Site Scripting vulnerability was reported in the 'phpinfo()' PHP function due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an integer overflow vulnerability was reported in 'pcrelib' due to an error, which could let a remote malicious user corrupt memory.</p> <p>Upgrades available at: <a href="http://www.php.net/get/php-4.4.1.tar.gz">http://www.php.net/get/php-4.4.1.tar.gz</a></p> <p>There is no exploit code required.</p>	<p>PHP Multiple Vulnerabilities <a href="#">CVE-2005-3388</a> <a href="#">CVE-2005-3389</a> <a href="#">CVE-2005-3390</a> <a href="#">CVE-2005-3391</a> <a href="#">CVE-2005-3392</a></p>	<p>Medium</p>	<p>Secunia Advisory: SA17371, October 31, 2005</p>
<p>phpBB Group phpBB 2.0.17 &amp; prior</p>	<p>Multiple vulnerabilities have been reported due to improper deregistration of global variables, which could let a remote malicious user conduct Cross-Site Scripting, execute arbitrary PHP code, or perform SQL injection.</p> <p>Upgrades available at: <a href="http://www.phpbb.com/files/releases/phpbb">http://www.phpbb.com/files/releases/phpbb</a></p>	<p>phpBB Deregistration Global Variables <a href="#">CVE-2005-3415</a></p>	<p>Medium</p>	<p>Security Focus, Bugtraq ID: 15243, October 31, 2005</p>

[2.0.17 to 2.0.18.zip](#)

There is no exploit code required.

PHPCafe Tutorial Manager PHPCafe Tutorial Manager	An SQL injection vulnerability has been reported in 'index.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 has been published.	PHPCafe Tutorial Manager SQL Injection  <a href="#">CVE-2005-3478</a>	Medium	Security Focus, Bugtraq ID: 15244, October 31, 2005
phpESP phpESP 1.7.5, -dev3, -dev2, -dev	A vulnerability has been reported in phpESP that could let remote malicious users conduct Cross-Site Scripting or SQL injection.  Upgrade to version 1.8-rc1: <a href="http://sourceforge.net/projects/phpesp/">http://sourceforge.net/projects/phpesp/</a>  There is no exploit code required.	phpESP Cross-Site Scripting & SQL Injection  <a href="#">CVE-2005-3406</a> <a href="#">CVE-2005-3407</a>	Medium	Secunia, Advisory: SA17333, October 28, 2005
PHP-Nuke PHP-Nuke Search Enhanced Module 1.1, 2.0	A vulnerability has been reported in PHP-Nuke Search Enhanced Module 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, Proof of Concept exploits have been published.	PHP-Nuke Cross-Site Scripting  <a href="#">CVE-2005-3368</a>	Medium	Secunia, Advisory: SA17296, October 27, 2005
Ringtail CaseBook 6.x	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'login.asp' due to insufficient sanitization of the 'user' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because different error responses are returned depending on whether or not a valid username is supplied, which could let a remote malicious user obtain sensitive information.  The vulnerabilities have reportedly been fixed in version 2005.  Currently we are not aware of any exploits for these vulnerabilities.	Ringtail CaseBook Cross-Site Scripting & Information Disclosure  <a href="#">CVE-2005-3479</a> <a href="#">CVE-2005-3480</a>	Medium	Secunia Advisory: SA17383, November 1, 2005
Snitz Communications Snitz Forums 2000, 3.4 .05	A Cross-Site Scripting vulnerability has been reported in 'post.asp' due to insufficient sanitization of the 'type' 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, a Proof of Concept exploit has been published.	Snitz Forum Cross-Site Scripting  <a href="#">CVE-2005-3411</a>	Medium	Security Focus, Bugtraq ID: 15241, October 31, 2005
Subdramer Subdramer 2.2.1	Multiple vulnerabilities have been reported in Subdramer that could let remote malicious users perform SQL injection.  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.	Subdramer SQL Injection  <a href="#">CVE-2005-3423</a>	Medium	Security Focus, ID: 15238, October 29, 2005
Thomas Rybak MG2 0.5.1	A vulnerability has been reported in MG2 that could let remote malicious users bypass authentication.  No workaround or patch available at time of publishing.  There is no exploit code required; however, Proof of Concept exploits have been published.	MG2 Authentication Bypassing  <a href="#">CVE-2005-3432</a>	Medium	Security Focus, ID: 15235, October 29, 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 a remote malicious user execute arbitrary HTML and script code.  Upgrades available at: <a href="http://prdownloads.sourceforge.net/tikiwiki/tikiwiki-1.9.1.1.tar.gz">http://prdownloads.sourceforge.net/tikiwiki/tikiwiki-1.9.1.1.tar.gz</a>  <b>Gentoo:</b> <a href="http://security.gentoo.org/glsa/glsa-200510-23.xml">http://security.gentoo.org/glsa/glsa-200510-23.xml</a>  There is no exploit code required.	TikiWiki Unspecified Cross-Site Scripting  <a href="#">CVE-2005-3283</a>	Medium	Security Tracker Alert ID: 1015087, October 20, 2005  <b>Gentoo Linux Security Advisory, GLSA 200510-23, October 28, 2005</b>

Wolflab Burning Board 2.5	Multiple vulnerabilities have been reported in Wolflab Burning Board Database Module, that could let remote malicious users perform SQL Injection.  No workaround or patch available at time of publishing.  Currently we are not aware of any exploits for this vulnerability.	Wolflab Burning Board SQL Injection  <a href="#">CVE-2005-3369</a>	Medium	Secunia Advisory: SA17347, October 27, 2005
------------------------------	---	--	--------	---

[back to top](#)

## Wireless

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

- IPTV Set For Massive Growth Spurt: Survey: According to a study by Analysis International, IPTV will become the next global growth industry. The China IPTV market, in particular, will skyrocket, reaching 16.7 billion RMB in revenue and nearly 17 million users by 2009. The early stages of market cultivation may pose some threats and risks, the group says. Uncertain regulations, insufficient hardware platforms, an immature value chain and unclear business models are the main concerns right now. Source: <http://www.networkingpipeline.com/showArticle.jhtml?articleID=173400478>.

### Wireless Vulnerabilities

- Nothing significant to report.

[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 (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
November 2, 2005	multispoof-0.7.0.tar.gz	N/A	An application that exploits weak, address based authentication that is frequently implemented by ISPs in Ethernet networks.
November 2, 2005	snort_bo_overflow_win32.pm.txt	Yes	Exploit for the Snort Back Orifice Preprocessor Remote Buffer Overflow vulnerability.
November 2, 2005	up-imaproxy-exp.txt	Yes	Proof of Concept exploit for the Imaproxy Format String vulnerability.
November 2, 2005	vubbXSS.txt	No	Exploit details for the VUBB VUBB Cross-Site Scripting & Path Disclosure vulnerabilities.
November 1, 2005	0510-exploits.tgz	N/A	New Packet Storm exploits for October, 2005.
October 31, 2005	backoffice_mult_exp.pl	No	Proof of Concept exploit for the Comersus BackOffice Multiple Input Validation And Information Disclosure vulnerabilities.
October 31, 2005	ethereal_slimp3_bof.py.txt	Yes	A Denial of Service exploit for the SLIMP3 protocol dissector vulnerability.
October 31, 2005	VERITAS-Linux.pl.txt VERITAS-Win32.pl.txt VERITAS-OSX.pl.txt	Yes	Exploits for the VERITAS NetBackup Arbitrary Code Execution vulnerability.
October 31, 2005	XH-Hasbani-HTTPD-DoS.c	No	Script that exploits the Hasbani Web Server Denial of Service vulnerability.
October 30, 2005	cirt-39-advisory.pdf	Yes	Exploitation details for the Novell ZENworks Patch Management SQL Injection vulnerability.
October 30, 2005	MS05-047-DoS.c	Yes	Remote Denial of Service exploit for the Microsoft Windows Plug and Play Arbitrary Code Execution vulnerability.
October 30, 2005	PBLang465.txt	No	Exploitation details for the PBLang Multiple Cross-Site Scripting Vulnerabilities.
October 30, 2005	vCard29.txt	No	Exploitation details for the Belchior Foundry VCard Remote File Include vulnerability.
October 29, 2005	subdreamer_sql.pl	No	Proof of Concept exploit for the Subdreamer Multiple Remote SQL Injection vulnerabilities.
October 27, 2005	advisory-103.txt	No	Proof of Concept exploit for the Techno Dreams Multiple Product SQL Injection vulnerability.
October 27, 2005	flysprayXSS.txt	No	Exploitation details for the Flyspray Multiple Cross-Site Scripting vulnerability.
October 27, 2005	msn-cap.c	N/A	A simple libpcap based MSN protocol sniffer.
October 27, 2005	mybbpr2.pl.txt	No	Proof of Concept exploit script for the MyBulletinBoard SQL Injection vulnerability.
October 27, 2005	nklan.pl	No	Exploit for the Nuked Klan Multiple Cross-Site Scripting & SQL Injection vulnerability.

October 27, 2005	php.4.4.1.txt	Yes	Exploit for the php 4.4.1 .htaccess apache DOS vulnerability.
October 27, 2005	php-iCalendar.txt	No	Exploitation details for the PHP ICalendar Remote File Include vulnerability.
October 27, 2005	phpnuke78sql.txt	No	Proof of Concept exploit for the PHPNuke Multiple Modules SQL Injection Vulnerabilities.
October 27, 2005	saphpLesson.txt	No	Exploit details for the SaphpLesson SQL Injection vulnerability.
October 26, 2005	mwchat.txt	No	Exploit for the MWChat SQL Injection vulnerability.
October 26, 2005	phpBB-IE-gif.txt	Yes	Exploit for the phpBB Cross-Site Scripting vulnerability.
October 26, 2005	UMPNPMGR.c	Yes	Proof of Concept exploit for the Microsoft Windows Plug and Play Arbitrary Code Execution vulnerability.

[\[back to top\]](#)

## Trends

- US-CERT is aware of publicly available Proof of Concept code for an Oracle worm. Currently, US-CERT cannot confirm if this code works but they are working with Oracle to determine the threat posed by this code.
- US-CERT is aware of publicly available exploit code for a buffer overflow vulnerability in the Snort Back Orifice preprocessor. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary code, possibly with root or SYSTEM privileges.
- **Your Next IM Could Be Your Network's Last:** According to data that was collected by IMlogic, the number of instant messaging oriented attacks rose by 30 percent over September when compared to last year. October 2005 counted 1300 percent more threats than the same month in 2004. This will eventually lead to an automated worm that will strike hundreds of thousands of machines in seconds.  
Source: <http://www.techweb.com/wire/security/173401244>
- **Barrage of Viruses Hits in October:** Sophos reports 1,685 new viruses and variants came out in October. Central Command also reports big numbers for October. There were a record number of viruses that hit the Internet in October but, but none of them were wide-spread and dangerous. Source: <http://www.esecurityplanet.com/trends/article.php/3560696>.
- **Rootkit-Armed Worm Attacking AIM:** According to FaceTime, a worm spreading through America Online's Instant Messenger (AIM) network carries a dangerous rootkit, code designed to hide a hacker's work from anti-virus scanners. Sdbot.add includes the "lockx.exe" rootkit. Source: <http://www.informationweek.com/story/showArticle.jhtml?articleID=172901455>.
- **Anti-Spyware Group Publishes Guidelines:** The Anti-Spyware Coalition has released guidelines to help consumers assess products designed to combat unwanted programs that sneak onto computers. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/10/27/AR2005102700819.html>.
- **Spammers exploit bird flu fears:** Sophos has reported a large increase in emails that offer online purchases of Tamiflu, the only know medicine that deals with the human version of the avian flu. Source: <http://www.itweek.co.uk/vnunet/news/2144878/spammers-bird-flu>.

[\[back to top\]](#)

## 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 folders.
2	Mytob-BE	Win32 Worm	Increase	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 anti virus, and modifying data.
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-GH	Win32 Worm	New	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
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	Netsky-Z	Win32 Worm	Increase	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.
7	Lovgate.w	Win32 Worm	Decrease	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.

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	Zafi-B	Win32 Worm	Decrease	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.
10	Mytob.C	Win32 Worm	Decrease	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.

Table updated November 1, 2005

[\[back to top\]](#)

**Last updated November 04, 2005**