

**US-CERT**

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Search US-CERT



Advanced Options...

## National Cyber Alert System

### Cyber Security Bulletin SB06-054

[Archive](#)

## Summary of Security Items from February 16 through February 22, 2006

The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should not be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

### Vulnerabilities

- Windows Operating Systems
  - [Avaya Products WMF Image Parsing Vulnerability](#)
  - [ViRobot Information Disclosure or Unauthorized Access](#)
  - [IBM Lotus Notes Multiple Vulnerabilities](#)
  - [Macallan Mail Solution Information Disclosure](#)
  - [Microsoft Internet Explorer Denial of Service or Arbitrary Code Execution](#)
  - [NJStar Chinese/Japanese Word Processor Arbitrary Code Execution](#)
  - [MailSite Denial of Service](#)
  - [Safe'n'Sec Privilege Elevation](#)
  - [Internet Anywhere EMailServer Denial of Service or Arbitrary Code Execution](#)
  - [WPCeasy SQL Injection Vulnerability](#)
- Unix/ Linux Operating Systems
  - [Apple Mac OS X Archive Metadata Arbitrary Command Execution](#)
  - [BlueZ Project hcidump Bluetooth L2CAP Remote Denial of Service \(Updated\)](#)
  - [Fetchmail 'fetchmailconf' Information Disclosure \(Updated\)](#)
  - [Fetchmail Remote Denial of Service \(Updated\)](#)
  - [LibAST Buffer Overflow \(Updated\)](#)
  - [GNU Tar PAX Remote Buffer Overflow](#)
  - [GnuPG Detached Signature Verification Bypass](#)
  - [KDE kjs UTF-8 Encoded URI Buffer Overflow \(Updated\)](#)
  - [LibTIFF TIFFOpen Remote Buffer Overflow \(Updated\)](#)
  - [Melange Chat Information Disclosure](#)
  - [Metamail Remote Buffer Overflow \(Updated\)](#)
  - [Micromuse Netcool/Neusecure Information Disclosure](#)
  - [Mozilla Bugzilla SQL Injection](#)
  - [Mozilla Bugzilla Information Disclosure](#)
  - [Multiple Vendors Xpdf Buffer Overflows \(Updated\)](#)
  - [Multiple Vendors OpenSSH SCP Shell Command Execution \(Updated\)](#)
  - [Multiple Vendors Linux Kernel Find Target Local Denial of Service \(Updated\)](#)
  - [Multiple Vendors Heimdal TelnetD Remote Denial of Service](#)
  - [Multiple Vendors Linux Kernel Stack Fault Exceptions Denial of Services \(Updated\)](#)
  - [Multiple Vendors Sudo Python Environment Cleaning Security Bypass \(Updated\)](#)
  - [Multiple Vendors Geeklog SQL Injection & File Inclusion](#)
  - [Multiple Vendors KPdf & KWord Multiple Unspecified Buffer & Integer Overflow \(Updated\)](#)
  - [Multiple Vendors Linux Kernel Denial of Service \(Updated\)](#)
  - [Multiple Vendors Linux Kernel Remote Denial of Service \(Updated\)](#)
  - [Multiple Vendors Noweb Insecure Temporary File Creation \(Updated\)](#)
  - [Multiple Vendors GnuTLS libtasn1 DER Decoding Remote Denial of Service \(Updated\)](#)
  - [Multiple Vendors Fetchmail Remote Denial of Service \(Updated\)](#)
  - [Multiple Vendors Linux Kernel IPv6 FlowLabel Denial of Service \(Updated\)](#)
  - [Multiple Vendors Tin News Reader Buffer Overflow](#)
  - [Multiple Vendors Linux Kernel SDLA IOCTL Unauthorized Local Firmware Access \(Updated\)](#)
  - [Nathan Neulinger CGIWrap Information Disclosure](#)
  - [netpbm Arbitrary Code Execution \(Updated\)](#)
  - [PEAR::Auth Multiple Unspecified SQL Injection](#)
  - [PeriBLOG Multiple Vulnerabilities](#)
  - [Fedora Directory Server Admin Server Password Disclosure](#)

- [RedHat Fedora Directory Server LDAP Denials of Service](#)
- [Heimdal RSHD Server Elevated Privileges \(Updated\)](#)
- [SCO UnixWare Ptrace Elevated Privileges](#)
- [Siteframe Beaumont HTML Injection](#)
- [SUSE CASA Pam\\_Micasa Remote Buffer Overflow](#)
- [Multiple Operating Systems](#)
  - [ADODB Multiple Cross-Site Scripting](#)
  - [Apache Libapreq2 Remote Denial of Service](#)
  - [Blue Coat ProxySG Policy Error Rules Bypass](#)
  - [BomberClone Error Messages Buffer Overflow](#)
  - [Barracuda Directory Multiple HTML Injection](#)
  - [Calacode @Mail HTML Injection](#)
  - [CherryPy Directory Traversal](#)
  - [Clever Copy Private Message HTML Injection](#)
  - [CPG Dragonfly CMS Cross-Site Scripting & SQL Injection](#)
  - [devScripts Admbook Remote Arbitrary PHP Code Execution](#)
  - [PHP-Fusion Cross-Site Scripting](#)
  - [D-Link DWL-G700AP Remote Denial of Service](#)
  - [Dovecot Double Free Remote Denial of Service](#)
  - [DreamCost HostAdmin Remote File Include](#)
  - [E107 Website System HTML Injection](#)
  - [E-Blah HTML Injection](#)
  - [EmuLinker Remote Denial of Service](#)
  - [Ethereal OSPF Protocol Dissection Buffer Overflow \(Updated\)](#)
  - [Ethereal IRC & GTP Dissectors Remote Denial of Service \(Updated\)](#)
  - [PHPNuke SQL Injection](#)
  - [Coppermine Photo Gallery File Include](#)
  - [Guestbox Vulnerabilities](#)
  - [HTML::BBCode HTML Injection](#)
  - [ilchClan SQL Injection](#)
  - [InfoVista VistaPortal Directory Traversal & Input Validation](#)
  - [Kyocera 3830 Printer Unauthorized Access](#)
  - [Leif M. Wright's Blog Multiple Vulnerabilities](#)
  - [Mambo Unspecified System Compromise](#)
  - [MiniNuke CMS SQL Injection](#)
  - [Mozilla Thunderbird Remote Denial of Service](#)
  - [Mozilla Firefox HTML Parsing Remote Denial of Service](#)
  - [Mozilla Thunderbird IFRAME JavaScript Execution](#)
  - [My Blog BBCode HTML Injection](#)
  - [Ethereal Denial of Service \(Updated\)](#)
  - [Multiple Vendors PunkBuster Module Remote Format String](#)
  - [MyBB Cross-Site Scripting & SQL Injection](#)
  - [MySQL 'mysql\\_install\\_db' Insecure Temporary File Creation](#)
  - [PEAR LiveUser Unauthorized File Access](#)
  - [Noah's Classifieds Multiple Vulnerabilities](#)
  - [PHPNuke CAPTCHA Bypass](#)
  - [PostgreSQL Privilege Escalation & Denial of Service \(Updated\)](#)
  - [PostNuke Multiple Vulnerabilities](#)
  - [BirthSys Multiple SQL Injection](#)
  - [RunCMS Cross-Site Scripting](#)
  - [RunCMS SQL Injection](#)
  - [SAP Business Connector Arbitrary File Access & Spoofing](#)
  - [Snort Frag3 Processor Intrusion Detection Bypass](#)
  - [SquirrelMail Multiple Cross-Site Scripting & IMAP Injection](#)
  - [Squishdot Mail Header Injection](#)
  - [Teca Scripts Guestex Input Validation](#)
  - [Teca Scripts Quirex Information Disclosure](#)
  - [Teca Diary Personal Edition SQL Injection](#)
  - [V-webmail Cross-Site Scripting & Information Disclosure](#)
  - [WebSPELL SQL Injection](#)
  - [Wimpy MP3 Player Text File Overwrite](#)
  - [Xerox ESS/ Network Controller and MicroServer Vulnerabilities](#)
  - [Xpdf PDF Splash Remote Buffer Overflow \(Updated\)](#)

[Wireless Trends & Vulnerabilities](#)

[General Trends](#)

[Viruses/Trojans](#)

## Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

### The Risk levels are defined below:

**High** - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

**Medium** - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

**Low** - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

*Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConflImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.*

Windows Operating Systems Only				
Vendor & Software Name	Description	Common Name	CVSS	Resources
Avaya Various Windows Products	Multiple potential vulnerabilities have been reported in various Avaya products, which run on the Windows platform, in response to Microsoft Security Advisories MS06-004, MS06-005, MS06-006, MS06-007, MS06-008, MS06-009, and MS06-010.  <a href="#">Avaya</a>  Currently we are not aware of any exploits for these vulnerabilities.	Avaya Products WMF Image Parsing Vulnerability  <a href="#">CVE-2006-0004</a> <a href="#">CVE-2006-0006</a> <a href="#">CVE-2006-0008</a> <a href="#">CVE-2006-0013</a> <a href="#">CVE-2006-0020</a> <a href="#">CVE-2006-0021</a>	<b>7</b> (CVE-2006-0020)	Avaya, ASA-2006-047, February 14, 2006
Hauri ViRobot	A vulnerability has been reported in ViRobot that could let remote malicious users disclose information or obtain unauthorized access.	ViRobot Information Disclosure or Unauthorized Access	Not Available	Security Tracker, Alert ID: 1015658, February 22, 2006

	<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>IBM</p> <p>Lotus Notes 6.x, 7.x</p>	<p>Multiple vulnerabilities have been reported: a vulnerability was reported in 'kvarcve.dll' when constructing the full pathname of a compressed file to check for its existence before extracting it from a ZIP archive, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in 'uudrdr.dll' when handling 'UUE' files that contain an encoded file with an overly long filename, which could let a remote malicious user execute arbitrary code; a Directory Traversal vulnerability was reported in 'kvarcve.dll' when generating the preview of a compressed file from ZIP, UUE, and TAR archives, which could let a remote malicious user delete arbitrary files; a vulnerability was reported in the 'TAR' reader when extracting files from a TAR archive that contain a long filename, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the HTML speed reader due to a boundary error,</p>	<p>IBM Lotus Notes Multiple Vulnerabilities</p> <p><a href="#">CVE-2005-2618</a> <a href="#">CVE-2005-2619</a></p>	<p>Not Available</p>	<p>Secunia Advisory: SA16280, February 10, 2006</p> <p><a href="#">US-CERT VU#884076</a></p> <p><b>Security Tracker, Alert ID: 1015657, February 21, 2006</b></p>

	<p>which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in the HTML speed reader when checking if a link references a local file due to a boundary error, which could let a remote malicious user execute arbitrary code.</p> <p>These issues have been addressed in Lotus Notes versions 6.5.5 and 7.0.1. Please contact the vendor to obtain fixes.</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p> <p><b>Entry was originally, erroneously listed as multiple OS.</b></p>			
Macallan Mail Solution 4.8.03.025	<p>An input validation vulnerability has been reported in Macallan Mail Solution that could let remote malicious users disclose information.</p> <p><a href="#">Macallan Mail Solution 4.8.05.004</a></p> <p>There is no exploit code required.</p>	<p>Macallan Mail Solution Information Disclosure</p> <p><a href="#">CVE-2006-0798</a></p>	<a href="#">2.8</a>	<p>Security Tracker, Alert ID: 1015647, February 20, 2006</p>
Microsoft Internet Explorer 6.0, 6.0 SP1	<p>A buffer overflow vulnerability has been reported in Internet Explorer that could let remote malicious users to cause a Denial of Service or execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	<p>Microsoft Internet Explorer Denial of Service or Arbitrary Code Execution</p> <p><a href="#">CVE-2006-0830</a></p>	<a href="#">Z</a>	<p>Security Focus, ID: 16687, February 16, 2006</p>

<p>NJStar Software</p> <p>Chinese/ Japanese Word Processor 5.01.41108 and prior</p>	<p>A buffer overflow vulnerability has been reported in Chinese/ Japanese Word Processor that could let remote malicious users execute arbitrary code.</p> <p><a href="#">Chinese/ Japanese Word Processor 5.10</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>NJStar Chinese/Japanese Word Processor Arbitrary Code Execution</p> <p><a href="#">CVE-2006-0807</a></p>	<p><a href="#">3.9</a></p>	<p>Security Tracker, Alert ID: 1015649, February 21, 2006</p>
<p>Rockliffe</p> <p>MailSite 4.2.1, 5, 5.3.4, 6.1.22 7.031</p>	<p>A vulnerability has been reported in MailSite, LDAP Service, that could let remote malicious users cause a Denial of Service.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>MailSite Denial of Service</p> <p><a href="#">CVE-2006-0790</a></p>	<p><a href="#">2.3</a></p>	<p>Secunia, Advisory: SA18888, February 15, 2006</p>
<p>Starforce</p> <p>Safe'n'Sec Personal 2.0</p>	<p>A vulnerability has been reported in Safe'n'Sec that could let local malicious users obtain elevated privileges.</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>Safe'n'Sec Privilege Elevation</p>	<p>Not Available</p>	<p>Security Focus, ID: 16762, February 21, 2006</p>
<p>True North Software</p> <p>Internet Anywhere EMailServer Corporate Edition 5.3.4</p>	<p>A buffer overflow vulnerability has been reported in Internet Anywhere EMailServer Corporate Edition that could let remote malicious users to cause a Denial of Service or execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are</p>	<p>Internet Anywhere EMailServer Denial of Service or Arbitrary Code Execution</p> <p><a href="#">CVE-2006-0853</a></p>	<p><a href="#">1.4</a></p>	<p>Security Focus, ID: 16744, February 21, 2006</p>

	not aware of any exploits for this vulnerability.			
WebPageCity WPCeasy	<p>A vulnerability has been reported in WPCeasy 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, a Proof of Concept exploit has been published.</p>	<p>WPCeasy SQL Injection Vulnerability</p> <p><a href="#">CVE-2006-0832</a></p>	<a href="#">7</a>	<p>Secunia, Advisory: SA18945, February 20, 2006</p>

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

UNIX / Linux Operating Systems Only				
Vendor & Software Name	Description	Common Name	CVSS	Resources
Apple Mac OS X Server 10.4.5, OS X 10.4.5	<p>A vulnerability has been reported in Apple Safari when processing file association meta data stored in the '_MACOSX' folder in ZIP archives, which could let a remote malicious user execute arbitrary commands.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit script, safari_safefiles_exec.pm, has been published.</p>	<p>Apple Mac OS X Archive Metadata Arbitrary Command Execution</p> <p><a href="#">CVE-2006-0848</a></p>	<a href="#">3.9</a>	<p>Secunia Advisory: SA18963, February 21, 2006</p> <p><a href="#">Cyber Security Alert SA06-053A</a></p> <p><a href="#">Technical Cyber Security Alert TA06-053A</a></p> <p><a href="#">US-CERT VU#999708</a></p>
BlueZ Project hcidump 1.29	<p>A remote Denial of Service vulnerability has been reported in 'l2cap.c' due to an error when handling L2CAP (Logical Link Control and Adaptation Layer Protocol) layer.</p> <p><a href="#">Ubuntu</a></p> <p>A Proof of Concept exploit script, hcidump-crash.c, has been published.</p>	<p>hcidump Bluetooth L2CAP Remote Denial of Service</p> <p><a href="#">CVE-2006-0670</a></p>	<a href="#">2.3</a>	<p>Secunia Advisory: SA18741, February 8, 2006</p> <p><b>Ubuntu Security Notice, USN-256-1, February 21, 2006</b></p>
Eric S Raymond Fetchmail 6.x	<p>A vulnerability has been reported in the 'fetchmailconf'</p>	<p>Fetchmail 'fetchmailconf' Information</p>	<a href="#">2.3</a>	<p>fetchmail-SA-2005-02 Security Announcement, October 21, 2005</p>

	<p>configuration utility due to a race condition, which could let a malicious user obtain sensitive information.</p> <p><a href="#">Upgrades available</a></p> <p><a href="#">Gentoo</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Slackware</a></p> <p>There is no exploit code required.</p>	<p>Disclosure</p> <p><a href="#">CVE-2005-3088</a></p>		<p>Gentoo Linux Security Advisory, GLSA 200511-06, November 6, 2005</p> <p>Ubuntu Security Notice, USN-215-1, November 07, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2005:209, November 10, 2005</p> <p>Debian Security Advisory, DSA 900-2 &amp; 900-3, November 21 &amp; 22, 2005</p> <p><b>Slackware Security Advisory, SSA:2006-045-01, February 14, 2006</b></p>
<p>Erik S. Raymond</p> <p>Fetchmail 6.3.0 - prior to 6.3.2</p>	<p>A remote Denial of Service vulnerability has been reported due to incorrect freeing of an invalid pointer when bouncing a message to the originator or to the local postmaster.</p> <p><a href="#">Update available</a></p> <p><a href="#">Slackware</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Fetchmail Remote Denial of Service</p> <p><a href="#">CVE-2006-0321</a></p>	<p><a href="#">2.3</a></p>	<p>Fetchmail Security Advisory, fetchmail-SA-2006-01, January 22, 2006</p> <p><b>Slackware Security Advisory, SSA:2006-045-01, February 14, 2006</b></p>
<p>ETERM</p> <p>LibAST prior to 0.7</p>	<p>A buffer overflow vulnerability has been reported in 'conf.c' due to a boundary error in the 'conf_find_file()' function, which could let a malicious user execute arbitrary code.</p> <p><a href="#">Update available</a></p> <p><a href="#">Gentoo</a></p> <p><a href="#">Debian</a></p> <p>An exploit script, eterm-exploit.c, has been published.</p>	<p>LibAST Buffer Overflow</p> <p><a href="#">CVE-2006-0224</a></p>	<p><a href="#">4.9</a></p>	<p>Secunia Advisory: SA18586, January 25, 2006</p> <p>Gentoo Linux Security Advisory, GLSA 200601-14, January 29, 2006</p> <p><b>Debian Security Advisory, DSA-976-1, February 15, 2006</b></p>
<p>GNU</p> <p>tar 1.15.90, 1.15.1, 1.14.90, 1.15, 1.14</p>	<p>A buffer overflow vulnerability has been reported when handling PAX extended headers due to a boundary error, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.</p>	<p>GNU Tar PAX Remote Buffer Overflow</p> <p><a href="#">CVE-2006-0300</a></p>	<p>Not available</p>	<p>Secunia Advisory: SA18973, February 22, 2006</p> <p>Mandriva Security Advisory, MDKSA-2006:046, February 21, 2006</p> <p>Ubuntu Security Notice,</p>

	<p><a href="#">GNU</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Ubuntu</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>			USN-257-1, February 23, 2006
GnuPG GnuPG / gpg prior to 1.4.2.1	<p>A vulnerability has been reported because 'gpgv' exits with a return code of 0 even if the detached signature file did not carry any signature (if 'gpgv' or "gpg --verify" is used), which could let a remote malicious user bypass security restrictions.</p> <p><a href="#">Patches available</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Gentoo</a></p> <p><a href="#">SuSE</a></p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>GnuPG Detached Signature Verification Bypass</p> <p><a href="#">CVE-2006-0455</a></p>	<a href="#">4.9</a>	<p>GnuPG Advisory, February 15, 2006</p> <p><b>Fedora Update Notification, FEDORA-2006-116, February 17, 2006</b></p> <p><b>Debian Security Advisory, DSA-978-1, February 17, 2006</b></p> <p><b>Mandriva Security Advisory, MDKSA-2006:043, February 17, 2006</b></p> <p><b>Ubuntu Security Notice, USN-252-1, February 17, 2006</b></p> <p><b>Gentoo Linux Security Advisory, GLSA 200602-10, February 18, 2006</b></p> <p><b>SuSE Security Announcement, SUSE-SA:2006:009, February 20, 2006</b></p>
KDE KDE 3.2.0 up to including 3.5.0	<p>A buffer overflow vulnerability has been reported in 'kjs' in the decoding of UTF-8 encoded URI sequences, which could let a remote malicious user execute arbitrary code.</p> <p><a href="#">Patch information</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Debian</a></p> <p><a href="#">SuSE</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">Gentoo</a></p> <p><a href="#">Slackware</a></p>	<p>KDE kjs UTF-8 Encoded URI Buffer Overflow</p> <p><a href="#">CVE-2006-0019</a></p>	<a href="#">7</a>	<p>KDE Security Advisory, January 19, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0184-11, January 19, 2006</p> <p>Ubuntu Security Notice, USN-245-1, January 20, 2006</p> <p>Debian Security Advisory, DSA-948-1, January 20, 2006</p> <p>SUSE Security Announcement, SUSE-SA:2006:003, January 20, 2006</p> <p>Mandriva Security Advisory, MDKSA-2006:019, January 20, 2006</p> <p>Gentoo Linux Security Advisory, GLSA</p>

	Currently we are not aware of any exploits for this vulnerability.			200601-11, January 22, 2006  <b>Slackware Security Advisory, SSA:2006-045-05, February 14, 2006</b>
LibTIFF  LibTIFF 3.4, 3.5.1-3.5.5, 3.5.7, 3.6 .0, 3.6.1, 3.7, 3.7.1	A buffer overflow vulnerability has been reported in the 'TIFFOpen()' function when opening malformed TIFF files, which could let a remote malicious user execute arbitrary code.  <a href="#">Patches available</a>  <a href="#">Gentoo</a>  <a href="#">Ubuntu</a>  <a href="#">SuSE</a>  <a href="#">TurboLinux</a>  <a href="#">Debian</a>  <a href="#">SCO</a>  <a href="#">SCO</a>  <a href="#">Mandriva</a>  Currently we are not aware of any exploits for this vulnerability.	LibTIFF TIFFOpen Remote Buffer Overflow  <a href="#">CVE-2005-1544</a> <a href="#">CVE-2005-1472</a>	<a href="#">7</a> (CVE-2005-1544)  <a href="#">2.3</a> (CVE-2005-1472)	Gentoo Linux Security Advisory, GLSA 200505-07, May 10, 2005  Ubuntu Security Notice, USN-130-1, May 19, 2005  SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005  Turbolinux Security Advisory, TLSA-2005-72, June 28, 2005  Debian Security Advisory, DSA 755-1, July 13, 2005  SCO Security Advisory, SCOSA-2005.34, September 19, 2005  SCO Security Advisory, SCOSA-2006.3, January 3, 2006  <b>Mandriva Security Advisory, MDKSA-2006:042, February 17, 2006</b>
Melange  Melange Chat System 1.10	A vulnerability has been reported due to a failure to properly secure HTTP request data, which could let a remote malicious user obtain sensitive information.  No workaround or patch available at time of publishing.  There is no exploit code required.	Melange Chat Information Disclosure	Not Available	Security Focus, Bugtraq ID: 16747, February 21, 2006
Metamail  Metamail 2.7	A buffer overflow vulnerability has been reported when handling boundary headers within email messages, which could let a remote malicious user execute arbitrary code. <b>Note: According to Security Tracker this is a Linux/Unix vulnerability. Previously classified as multiple operating</b>	Metamail Remote Buffer Overflow  <a href="#">CVE-2006-0709</a>	<a href="#">2.3</a>	Security Focus, Bugtraq ID: 16611, February 13, 2006  <b>RedHat Security Advisory, RHSA-2006:0217-4, February 21, 2006</b>  <b>Mandriva Security Advisory, MDKSA-2006:047, February 22, 2006</b>

	<p><b>systems.</b></p> <p><a href="#">RedHat</a></p> <p><a href="#">Mandriva</a></p> <p>A Proof of Concept exploit has been published.</p>			
<p>Micromuse</p> <p>Netcool/Neusecure 3.0.236 -1</p>	<p>Several vulnerabilities have been reported: a vulnerability was reported because passwords are stored in cleartext in configuration files, which could let a malicious user obtain sensitive information; and a vulnerability was reported in the database connection log in the default configuration because it is readable by all users, which could let a malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code.</p>	<p>Micromuse Netcool/ Neusecure Information Disclosure</p> <p><a href="#">CVE-2006-0837</a> <a href="#">CVE-2006-0838</a></p>	<p><a href="#">1.6</a> (CVE-2006-0837)</p> <p><a href="#">1.6</a> (CVE-2006-0838)</p>	<p>Secunia Advisory: SA18922, February 17, 2006</p>
<p>Mozilla.org</p> <p>Bugzilla 2.17.1-2.21.1</p>	<p>An SQL injection vulnerability has been reported in 'editparams.cgi' due to insufficient validation of the 'whinedays' parameter, which could let a remote malicious user execute arbitrary SQL code.</p> <p><a href="#">Updates available</a></p> <p>There is no exploit code required.</p>	<p>Bugzilla SQL Injection</p>	<p>Not Available</p>	<p>Security Focus, Bugtraq ID: 16738, February 21, 2006</p>
<p>Mozilla.org</p> <p>Bugzilla 2.19.3, 2.20-2.21.2</p>	<p>A vulnerability has been reported in the login form on the home page due to a design error in the application, which could let a remote malicious user obtain sensitive information.</p> <p><a href="#">Updates available</a></p> <p>There is no exploit code required.</p>	<p>Bugzilla Information Disclosure</p>	<p>Not Available</p>	<p>Security Focus, Bugtraq ID: 16745, February 21, 2006</p>
<p>Multiple Vendors</p> <p>Xpdf 3.0 pl2 &amp; pl3, 3.0 1, 3.00, 2.0-2.03, 1.0 0, 1.0 0a, 0.90-0.93; RedHat Fedora Core4,</p>	<p>Multiple vulnerabilities have been reported: a heap-based buffer overflow vulnerability was reported in the 'DCTStream::read</p>	<p>Xpdf Buffer Overflows</p> <p><a href="#">CVE-2005-3191</a> <a href="#">CVE-2005-3192</a></p>	<p><a href="#">3.9</a> (CVE-2005-3191)</p> <p><a href="#">7</a> (CVE-2005-3192)</p>	<p>iDefense Security Advisory, December 5, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-1121 &amp;</p>

Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, 2.1, Enterprise Linux AS 4, AS 3, 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; teTeX 2.0.1, 2.0; Poppler poppler 0.4.2; KDE kpdf 0.5, KOffice 1.4.2 ; PDFTOHTML DFTOHTML 0.36

BaselineSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'DCTStream::read ProgressiveSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'StreamPredictor::StreamPredictor()' function in 'xpdf/Stream.cc' when using the 'numComps' value to calculate the memory size, which could let a remote malicious user potentially execute arbitrary code; and a vulnerability was reported in the 'JPXStream::readCodestream()' function in 'xpdf/JPXStream.cc' when using the 'nXTiles' and 'nYTiles' values from a PDF file to copy data from the file into allocated memory, which could let a remote malicious user potentially execute arbitrary code.

[Patches available](#)

[Fedora](#)

[RedHat](#)

[KDE](#)

[SUSE](#)

[Ubuntu](#)

[Gentoo](#)

[RedHat](#)

[RedHat](#)

[RedHat](#)

[Mandriva](#)

[Debian](#)

[CVE-2005-3193](#)

[3.9](#)  
(CVE-2005-3193)

1122, December 6, 2005

RedHat Security Advisory, RHSA-2005:840-5, December 6, 2005

KDE Security Advisory, advisory-20051207-1, December 7, 2005

SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005

Ubuntu Security Notice, USN-227-1, December 12, 2005

Gentoo Linux Security Advisory, GLSA 200512-08, December 16, 2005

RedHat Security Advisories, RHSA-2005:868-4, RHSA-2005:867-5 & RHSA-2005:878-4, December 20, 2005

Mandriva Linux Security Advisories MDKSA-2006:003-003-006, January 6, 2006

Debian Security Advisory, DSA-936-1, January 11, 2006

Debian Security Advisory, DSA-937-1, January 12, 2006

Debian Security Advisory, DSA 938-1, January 12, 2006

Fedora Update Notifications, FEDORA-2005-028 & 029, January 12, 2006

SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006

RedHat Security Advisory, RHSA-2006:0160-14, January 19, 2006

SUSE Security Summary Report, SUSE-SR:2006:002, January 20, 2006

SGI Security Advisory, 20051201-01-U, January

	<p><a href="#">Debian</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">SuSE</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">SGI</a></p> <p><a href="#">Debian</a></p> <p><a href="#">TurboLinux</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Slackware</a></p> <p><a href="#">Slackware</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>			<p>20, 2006</p> <p>Debian Security Advisory, DSA-950-1, January 23, 2006</p> <p>Turbolinux Security Advisory, TLISA-2006-2, January 25, 2006</p> <p>Debian Security Advisories, DSA-961-1 &amp; 962-1, February 1, 2006</p> <p><b>Slackware Security Advisories, SSA:2006-045-04 &amp; SSA:2006-045-09, February 14, 2006</b></p>
<p>Multiple Vendors</p> <p>OpenSSH 3.x, 4.x; RedHat Fedora Core3 &amp; Core4</p>	<p>A vulnerability has been reported in 'scp' when performing copy operations that use filenames due to the insecure use of the 'system()' function, which could let a malicious user obtain elevated privileges.</p> <p><a href="#">Fedora</a></p> <p><a href="#">Trustix</a></p> <p><a href="#">Patches available</a></p> <p><a href="#">OpenBSD</a></p> <p><a href="#">SuSE</a></p> <p><a href="#">Slackware</a></p> <p><a href="#">Gentoo</a></p> <p><a href="#">Ubuntu</a></p> <p>There is no exploit code required.</p>	<p>OpenSSH SCP Shell Command Execution</p> <p><a href="#">CVE-2006-0225</a></p>	<p><a href="#">4.9</a></p>	<p>Security Focus, Bugtraq ID: 16369, January 24, 2006</p> <p>Fedora Security Advisory, FEDORA-2006-056, January 24, 2006</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2006-0004, January 27, 2006</p> <p>Security Focus, Bugtraq ID: 16369, January 31, 2006</p> <p>Secunia Advisory: SA18798, February 13, 2006</p> <p>SUSE Security Announcement, SUSE-SA:2006:008, February 14, 2006</p> <p><b>Slackware Security Advisory, SSA:2006-045-06, February 14, 2006</b></p> <p><b>Gentoo Linux Security Advisory, GLSA 200602-11, February 20, 2006</b></p> <p><b>Ubuntu Security Notice, USN-255-1, February 21, 2006</b></p>
<p>Multiple Vendors</p> <p>RedHat Enterprise Linux WS 3, ES 3, AS</p>	<p>A Denial of Service vulnerability has been reported in the 'find_target' function due</p>	<p>Linux Kernel Find_Target Local Denial of</p>	<p><a href="#">2.3</a></p>	<p>Security Focus, Bugtraq ID: 14965, September 28, 2005</p>

<p>3, Desktop 3.0; Linux kernel 2.4-2.4.28</p>	<p>to a failure to properly handle unexpected conditions when attempting to handle a NULL return value from another function.</p> <p><a href="#">Upgrades available</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Mandriva</a></p> <p>There is no exploit code required.</p>	<p>Service</p> <p><a href="#">CVE-2005-2553</a></p>		<p>RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005</p> <p>Debian Security Advisory, DSA 921-1, December 14, 2005</p> <p><b>Mandriva Security Advisory, MDKSA-2006:044, February 21, 2006</b></p>
<p>Multiple Vendors</p> <p>Royal Institute of Technology Heimdal 0.7, 0.6- 0.6.5, 0.5.0-0.5.3, 0.4 a-f; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha; Ubuntu Ubuntu Linux 5.10 powerpc Ubuntu Ubuntu Linux 5.10 i386 Ubuntu Ubuntu Linux 5.10 amd64 Ubuntu Linux 5.0 4 powerpc, i386, amd6, 4.1 ppc, ia64, ia32</p>	<p>A remote Denial of Service vulnerability has been reported in 'telnetd' due to a NULL pointer dereference error.</p> <p>Update to version 0.7.2 or 0.6.6.</p> <p><a href="#">Debian</a></p> <p><a href="#">Ubuntu</a></p> <p>There is no exploit code required.</p>	<p>Heimdal TelnetD Remote Denial of Service</p> <p><a href="#">CVE-2006-0677</a></p>	<p><a href="#">3.3</a></p>	<p>Bugtraq ID: 16676, February 16, 2006</p> <p>Debian Security Advisory, DSA-977-1, February 16, 2006</p> <p>Ubuntu Security Notice, USN-253-1, February 17, 2006</p>
<p>Multiple Vendors</p> <p>SuSE Linux Professional 9.0, x86_64; Linux kernel 2.6-2.6.12, 2.5 .0- 2.5.69, 2.4-2.4.32</p>	<p>An unspecified Denial of Service vulnerability has been reported when stack fault exceptions are triggered.</p> <p><a href="#">SUSE</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Mandriva</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel Stack Fault Exceptions Denial of Service</p> <p><a href="#">CVE-2005-1767</a></p>	<p><a href="#">2.3</a></p>	<p>Security Focus, 14467, August 3, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005</p> <p>Ubuntu Security Notice, USN-187-1, September 25, 2005</p> <p>RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005</p> <p>Debian Security Advisories, DSA 921-1 &amp; 922-1, December 14, 2005</p> <p><b>Mandriva Security Advisory, MDKSA-2006:044, February 21, 2006</b></p>
<p>Multiple Vendors</p> <p>Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;</p>	<p>A vulnerability has been reported in the 'PYTHONINSPECT' variable, which could let a malicious user bypass security restrictions and obtain elevated</p>	<p>Sudo Python Environment Cleaning Security Bypass</p> <p><a href="#">CVE-2006-0151</a></p>	<p><a href="#">7</a></p>	<p>Security Focus, Bugtraq ID: 16184, January 9, 2006</p> <p>Security Focus, Bugtraq ID: 16184, January 12, 2006</p> <p>Debian Security Advisory,</p>

<p>Todd Miller Sudo 1.6-1.6.8, 1.5.6-1.5.9</p>	<p>privileges.</p> <p><a href="#">Todd Miller Sudo</a></p> <p><a href="#">AppleWebSharing Update</a></p> <p><a href="#">Conectiva</a></p> <p><a href="#">Debian</a></p> <p><a href="#">EnGarde</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">FreeBSD</a></p> <p><a href="#">GratiSoft Sudo</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">OpenPKG</a></p> <p><a href="#">OpenBSD</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Slackware</a></p> <p><a href="#">SuSE</a></p> <p><a href="#">Trustix</a></p> <p><a href="#">TurboLinux</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Wirex</a></p> <p><a href="#">Debian</a></p> <p><a href="#">SuSE</a></p> <p><a href="#">Slackware</a></p> <p>An exploit script, sudo_local_python_exploit.txt, has been published.</p>			<p>DSA-946-1, January 20, 2006</p> <p>SUSE Security Summary Report, SUSE-SR:2006:002, January 20, 2006</p> <p>Slackware Security Advisory, SSA:2006-045-08, February 14, 2006</p> <p><b>Slackware Security Advisory, SSA:2006-045-08, February 14, 2006</b></p>
<p>Multiple Vendors</p> <p>Geeklog prior to 1.3.11sr4 &amp; 1.4.0sr1; Media Gallery 1.2.3</p>	<p>Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'users.php' and 'lib-sessions.php' due to insufficient sanitization of cookies before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a file include vulnerability was reported in 'lib-common.php' due to insufficient verification of cookies before using to include files, which could let a remote malicious user execute arbitrary php code.</p>	<p>Geeklog SQL Injection &amp; File Inclusion</p> <p><a href="#">CVE-2006-0823</a></p> <p><a href="#">CVE-2006-0824</a></p>	<p><a href="#">7</a> (CVE-2006-0823)</p> <p><a href="#">7</a> (CVE-2006-0824)</p>	<p>Security Focus, Bugtraq ID: 16755, February 21, 2006</p>

	<p><a href="#">Media Gallery</a></p> <p><a href="#">Geeklog</a></p> <p>There is no exploit code required.</p>			
<p>Multiple Vendors</p> <p>KDE kword 1.4.2, kpdf 3.4.3, 3.2, KOffice 1.4-1.4.2, kdegraphics 3.4.3, 3.2; Gentoo Linux</p>	<p>Multiple buffer and integer overflows have been reported, which could let a remote malicious user execute arbitrary code.</p> <p><a href="#">Gentoo</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Debian</a></p> <p><a href="#">SuSE</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Trustix</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">SGI</a></p> <p><a href="#">Debian</a></p> <p><a href="#">TurboLinux</a></p> <p><a href="#">Gentoo</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Slackware</a></p> <p><a href="#">Slackware</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>KPdf &amp; KWord Multiple Unspecified Buffer &amp; Integer Overflow</p> <p><a href="#">CVE-2005-3624</a></p> <p><a href="#">CVE-2005-3625</a></p> <p><a href="#">CVE-2005-3626</a></p> <p><a href="#">CVE-2005-3627</a></p>	<p>Not Available</p>	<p>Gentoo Linux Security Advisory GLSA 200601-02, January 5, 2006</p> <p>Ubuntu Security Notice, USN-236-1, January 05, 2006</p> <p>Fedora Update Notifications, FEDORA-2005-000, January 5, 2006</p> <p>Mandriva Linux Security Advisories MDKSA-2006:003-003-006 &amp; 008, January 6 &amp; 7, 2006</p> <p>Ubuntu Security Notice, USN-236-2, January 09, 2006</p> <p>Debian Security Advisory DSA 931-1, January 9, 2006</p> <p>Debian Security Advisory, DSA-936-1, January 11, 2006</p> <p>SUSE Security Announcement, SUSE-SA:2006:001, January 11, 2006</p> <p>RedHat Security Advisories, RHSA-2006:0163-2 &amp; RHSA-2006:0177-5, January 11, 2006</p> <p>Fedora Update Notifications, FEDORA-2005-028 &amp; 029, January 12, 2006</p> <p>Debian Security Advisories, DSA 937-1, 938-1, &amp; 940-1, January 12 &amp; 13, 2006</p> <p>Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006</p> <p>Mandriva Linux Security Advisory, MDKSA-2006:012, January 13, 2006</p> <p>RedHat Security Advisory,</p>

				<p>RHSA-2006:0160-14, January 19, 2006</p> <p>SGI Security Advisory, 20051201-01-U, January 20, 2006</p> <p>Debian Security Advisory, DSA-950-1, January 23, 2006</p> <p>Turbolinux Security Advisory, TLSA-2006-2, January 25, 2006</p> <p>Gentoo Linux Security Advisory, GLSA 200601-17, January 30, 2006</p> <p>Debian Security Advisories, DSA-961-1 &amp; 962-1, February 1, 2006</p> <p><b>Slackware Security Advisories, SSA:2006-045-04 &amp; SSA:2006-045-09, February 14, 2006</b></p>
<p>Multiple Vendors</p> <p>Linux kernel 2.6-2.6.12.3, 2.4-2.4.32</p>	<p>A Denial of Service vulnerability has been reported in 'IP_VS_CONN_FLUSH' due to a NULL pointer dereference.</p> <p>Kernel versions 2.6.13 and 2.4.32-pre2 are not affected by this issue.</p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Conectiva</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Mandriva</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel Denial of Service</p> <p><a href="#">CVE-2005-3274</a></p>	<p><a href="#">2.3</a></p>	<p>Security Focus, Bugtraq ID: 15528, November 22, 2005</p> <p>Ubuntu Security Notice, USN-219-1, November 22, 2005</p> <p>Mandriva Linux Security Advisories, MDKSA-2005:219 &amp; 220, November 30, 2005</p> <p>Debian Security Advisory, DSA 922-1, December 14, 2005</p> <p>Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0190-5, February 1, 2006</p> <p><b>Mandriva Security Advisory, MDKSA-2006:044, February 21, 2006</b></p>
<p>Multiple Vendors</p> <p>Linux kernel 2.6-2.6.12, 2.4-2.4.31</p>	<p>A remote Denial of Service vulnerability has been reported due to a design error in the kernel.</p> <p>The vendor has released versions 2.6.13 and 2.4.32-rc1 of the kernel to address this issue.</p>	<p>Linux Kernel Remote Denial of Service</p> <p><a href="#">CVE-2005-3275</a></p>	<p><a href="#">3.3</a></p>	<p>Ubuntu Security Notice, USN-219-1, November 22, 2005</p> <p>Mandriva Linux Security Advisories, MDKSA-2005:218, 219 &amp; 220, November 30, 2005</p> <p>SUSE Security</p>

	<p><a href="#">Ubuntu</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">SUSE</a></p> <p><a href="#">Conectiva</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Mandriva</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>			<p>Announcement, SUSE-SA:2005:068, December 14, 2005</p> <p>Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006</p> <p>RedHat Security Advisories, RHSA-2006:0190-5 &amp; RHSA-2006:0191-9, February 1, 2006</p> <p><b>Mandriva Security Advisory, MDKSA-2006:044, February 21, 2006</b></p>
<p>Multiple Vendors</p> <p>Norman Ramsey Noweb 2.9 a, 2.10 c; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha</p>	<p>A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user overwrite critical files.</p> <p><a href="#">Debian</a></p> <p><a href="#">Ubuntu</a></p> <p>There is no exploit code required.</p>	<p>Noweb Insecure Temporary File Creation</p> <p><a href="#">CVE-2005-3342</a></p>	<p>Not Available</p>	<p>Debian Security Advisory, DSA-968-1, February 13, 2006</p> <p><b>Ubuntu Security Notice, USN-254-1, February 21, 2006</b></p>
<p>Multiple Vendors</p> <p>RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; GNU Libtasn1 prior to 1.2.10, GnuTLS prior to 1.2.10</p>	<p>A remote Denial of Service vulnerability has been reported due to improper decoding of DER encoded data. This could possibly lead to the execution of arbitrary code.</p> <p><a href="#">libtasn</a></p> <p><a href="#">gnutls</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Gentoo</a></p> <p><a href="#">Ubuntu</a></p> <p>A Proof of Concept exploit has been published.</p>	<p>GnuTLS libtasn1 DER Decoding Remote Denial of Service</p> <p><a href="#">CVE-2006-0645</a></p>	<p><a href="#">Z</a></p>	<p>Security Tracker Alert ID: 1015612, February 11, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0207-01, February 10, 2006</p> <p>Fedora Update Notification, FEDORA-2006-107, February 10, 2006</p> <p>Mandriva Security Advisory, MDKSA-2006:039, February 13, 2006</p> <p><b>Gentoo Linux Security Advisory, GLSA 200602-08, February 16, 2006</b></p> <p><b>Ubuntu Security Notice, USN-251-1, February 16, 2006</b></p>
<p>Multiple Vendors</p> <p>RedHat Fedora Core4, Core3; Eric Raymond</p>	<p>A remote Denial of Service vulnerability has been reported when Fetchmail is configured in 'multidrop' mode due</p>	<p>Fetchmail Remote Denial of Service</p>	<p><a href="#">3.3</a></p>	<p>Security Focus, Bugtraq ID: 15987, December 20, 2005</p> <p>Fedora Update Notifications</p>

<p>Fetchmail 6.3.0, 6.2.5 .4, 6.2.5 .2, 6.2.5.1, 6.2.5</p>	<p>to a failure to handle unexpected input.</p> <p><a href="#">Upgrades available</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Trustix</a></p> <p><a href="#">Slackware</a></p> <p>There is no exploit code required.</p>	<p><a href="#">CVE-2005-4348</a></p>		<p>FEDORA-2005-1186 &amp; 1187, December 20, 2005</p> <p>Mandriva Linux Security Advisory MDKSA-2005:236, December 23, 2005</p> <p>Ubuntu Security Notice, USN-233-1 January 02, 2006</p> <p>Debian Security Advisory, DSA 939-1, January 13, 2006</p> <p>Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006</p> <p><b>Slackware Security Advisory, SSA:2006-045-01, February 14, 2006</b></p>
<p>Multiple Vendors</p> <p>SuSE Linux Professional 10.0 OSS, 10.0, Personal 10.0 OSS; Linux kernel 2.6-2.6.13, Linux kernel 2.4-2.4.32</p>	<p>A Denial of Service vulnerability has been reported in FlowLable.</p> <p><a href="#">Upgrades available</a></p> <p><a href="#">SUSE</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Mandriva</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel IPv6 FlowLable Denial of Service</p> <p><a href="#">CVE-2005-3806</a></p>	<p><a href="#">5.3</a></p>	<p>Security Focus, Bugtraq ID: 15729, December 6, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005</p> <p>RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006</p> <p>Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006</p> <p>RedHat Security Advisories, RHSA-2006:0190-5 &amp; RHSA-2006:0191-9, February 1, 2006</p> <p><b>Mandriva Security Advisory, MDKSA-2006:044, February 21, 2006</b></p>
<p>Multiple Vendors</p> <p>Tin News Reader 1.8 &amp; prior ; OpenPKG 2.5, 2.4, 2.3, OpenPKG Current</p>	<p>A off-by-one buffer overflow vulnerability has been reported due to insufficient boundary checks on user-supplied data before using it in a finite-sized buffer, which</p>	<p>Tin News Reader Buffer Overflow</p> <p><a href="#">CVE-2006-0804</a></p>	<p><a href="#">Z</a></p>	<p>Security Focus, Bugtraq ID: 16728, February 20, 2006</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2006.005, February 19, 2006</p>

	<p>could let a remote malicious user execute arbitrary code.</p> <p><a href="#">Tin News Reader</a></p> <p><a href="#">OpenPKG</a></p> <p>There is no exploit code required.</p>			
<p>Multiple Vendors</p> <p>Ubuntu Linux 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.10, 2.4-2.4.28</p>	<p>A vulnerability has been reported in the SDLA driver, which could let a malicious user unauthorized access.</p> <p><a href="#">Updates available</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Mandriva</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel SDLA IOCTL Unauthorized Local Firmware Access</p> <p><a href="#">CVE-2006-0096</a></p>	<p><a href="#">4.9</a></p>	<p>Ubuntu Security Notice, USN-244-1 January 18, 2006</p> <p><b>Mandriva Security Advisory, MDKSA-2006:044, February 21, 2006</b></p>
<p>Nathan Neulinger</p> <p>CGIWrap 3.0, 2.0-2.7, 1.0</p>	<p>A vulnerability was reported because system information is disclosed in an error message when an error occurs during the execution of a script, which could let a remote malicious user obtain sensitive information. <i>Note: This occurs even when the '--with-quiet-errors' option is used.</i></p> <p><a href="#">updates available</a></p> <p>There is no exploit code required.</p>	<p>Nathan Neulinger CGIWrap Information Disclosure</p> <p><a href="#">CVE-2006-0767</a></p>	<p><a href="#">2.3</a></p>	<p>Security Focus, Bugtraq ID: 16669, February 15, 2006</p>
<p>netpbm 10.0</p>	<p>A vulnerability has been reported in netpbm ('-dSAFER') that could let malicious users execute arbitrary postscript code.</p> <p><a href="#">Trustix</a></p> <p><a href="#">Gentoo</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">SUSE</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">SGI</a></p> <p><a href="#">Conectiva</a></p> <p><a href="#">TurboLinux</a></p>	<p>netpbm Arbitrary Code Execution</p> <p><a href="#">CVE-2005-2471</a></p>	<p><a href="#">7</a></p>	<p>Secunia Advisory: SA16184, July 25, 2005</p> <p>Trustix Secure Linux Security Advisory, #2005-0038, July 29, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200508-04, August 5, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:133, August 10, 2005</p> <p>Ubuntu Security Notice, USN-164-1, August 11, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-727 &amp; 728, August 17, 2005</p>

	<p><a href="#">Fedora</a></p> <p><a href="#">Fedora</a></p> <p>There is no exploit code required.</p>			<p>SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005</p> <p>RedHat Security Advisory, RHSA-2005:743-08, August 22, 2005</p> <p>SGI Security Advisory, 20050901-01-U, September 7, 2005</p> <p>Conectiva Linux Announcement, CLSA-2005:1007, September 13, 2005</p> <p>Turbolinux Security Advisory, TLSA-2005-90, September 20, 2005</p> <p>Fedora Update Notification, FEDORA-2005-000, January 5, 2006</p> <p><b>Fedora Update Notification, FEDORA-2006-112, February 16, 2006</b></p>
<p>PEAR</p> <p>PEAR::Auth 1.2.4 &amp; prior to 1.3.0r4</p>	<p>Multiple unspecified SQL injection vulnerabilities have been reported due to insufficient sanitization , which could let a remote malicious user execute arbitrary SQL code.</p> <p><a href="#">Updates available</a></p> <p>There is no exploit code required.</p>	<p>PEAR::Auth Multiple Unspecified SQL Injection</p>	<p>Not Available</p>	<p>Security Focus, Bugtraq ID: 16758, February 21, 2006</p>
<p>Perl BLOG</p> <p>PerlBLOG 1.09b &amp; prior</p>	<p>Multiple vulnerabilities have been reported: a vulnerability was reported in 'weblog.ph' in the 'Post Comment' functionality due to insufficient sanitization of the 'reply' parameter, which could let a remote malicious user conduct script insertion attacks; a vulnerability was reported in 'weblog.ph' in the 'Archives' functionality due to insufficient sanitization of the 'month' parameter, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported in 'weblog.pl' due to insufficient sanitization of</p>	<p>PerlBLOG Multiple Vulnerabilities</p> <p><a href="#">CVE-2006-0780</a> <a href="#">CVE-2006-0781</a> <a href="#">CVE-2006-0782</a></p>	<p><a href="#">2.3</a> (CVE-2006-0780)</p> <p><a href="#">2.3</a> (CVE-2006-0781)</p> <p><a href="#">7</a> (CVE-2006-0782)</p>	<p>Security Focus, Bugtraq ID: 16707, February 17, 2006</p>

	<p>the 'name' and 'body' parameters, which could let a remote malicious user execute arbitrary script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>			
<p>RedHat</p> <p>Fedora Directory Server 1.0</p>	<p>A vulnerability has been reported because the Admin Server exposes the password, which could let a remote malicious user obtain sensitive information.</p> <p><a href="#">Update available</a></p> <p>There is no exploit code required.</p>	<p>Fedora Directory Server Admin Server Password Disclosure</p> <p><a href="#">CVE-2005-3630</a></p>	<p>Not Available</p>	<p>Secunia Advisory: SA18939, February 20, 2006</p>
<p>RedHat</p> <p>Fedora Directory Server 1.0</p>	<p>Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in the LDAP component when processing BER packets; a Denial of Service vulnerability was reported in the LDAP component in the 'dn2ancestor' code; and a Denial of Service vulnerability was reported in the LDAP component when processing BER packets when a specially crafted BER sequence is submitted.</p> <p><a href="#">Patches available</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>Fedora Directory Server LDAP Denials of Service</p> <p><a href="#">CVE-2006-0451</a> <a href="#">CVE-2006-0452</a> <a href="#">CVE-2006-0453</a></p>	<p>Not Available</p>	<p>Security Focus, Bugtraq ID: 16677, February 16, 2006</p>
<p>Royal Institute of Technology</p> <p>Heimdal prior to 0.6.6 &amp; 0.7.2</p>	<p>A vulnerability has been reported in the 'rshd' server when storing forwarded credentials due to an unspecified error, which could let a malicious user obtain elevated privileges.</p> <p>Update to version 0.7.2 or 0.6.6.</p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Debian</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Heimdal RSHD Server Elevated Privileges</p> <p><a href="#">CVE-2006-0582</a></p>	<p><a href="#">1.6</a></p>	<p>Security Tracker Alert ID: 1015591, February 7, 2006</p> <p>Ubuntu Security Notice, USN-247-1, February 09, 2006</p> <p><b>Debian Security Advisory, DSA-977-1, February 16, 2006</b></p>

<p>SCO</p> <p>Unixware 7.1.4, 7.1.3</p>	<p>A vulnerability has been reported in the 'ptrace()' system call due to an unspecified error, which could let a malicious user obtain elevated privileges.</p> <p><a href="#">Updates available</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>SCO UnixWare Ptrace Elevated Privileges</p> <p><a href="#">CVE-2005-2934</a></p>	<p>Not Available</p>	<p>SCO Security Advisory, SCOSA-2006.9, February 21, 2006</p>
<p>Siteframe</p> <p>Siteframe Beaumont 5.0.2, 5.0.1, 5.0.1a</p>	<p>An HTML injection vulnerability has been reported in 'page.php' due to insufficient sanitization, 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>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>Siteframe Beaumont HTML Injection</p> <p><a href="#">CVE-2006-0783</a></p>	<p><a href="#">2.3</a></p>	<p>Security Focus, Bugtraq ID: 16695, February 17, 2006</p>
<p>SuSE</p> <p>Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0</p>	<p>A buffer overflow vulnerability has been reported in 'Pam_Micasa', which could let a remote malicious user obtain superuser privileges.</p> <p><a href="#">Updates available</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>SUSE CASA Pam_Micasa Remote Buffer Overflow</p> <p><a href="#">CVE-2006-0736</a></p>	<p>Not Available</p>	<p>SUSE Security Announcement, SA:2006:010, February 22, 2006</p>

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

## Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
ADOdb ADOdb 4.71 & prior	<p>Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'adodb_pager.inc.php' due to insufficient sanitization of the 'next_page' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability was reported in 'adodb_pager.inc.php' due to the unsafe use of 'PHP_SELF,' 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>There is no exploit code required.</p>	<p>ADOdb Multiple Cross-Site Scripting</p> <p><a href="#">CVE-2006-0806</a></p>	<a href="#">2.3</a>	Secunia Advisory: SA18928, February 20, 2006
Apache Software Foundation libapreq2 2.0.6	<p>A remote Denial of Service vulnerability has been reported due to errors in the 'apreq_parse_headers()' and 'apreq_parse_urlencoded()' functions.</p> <p><a href="#">Update available</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Apache Libapreq2 Remote Denial of Service</p> <p><a href="#">CVE-2006-0042</a></p>	<a href="#">2.3</a>	Security Focus, Bugtraq ID: 16710, February 17, 2006
BlueCoat Systems Blue Coat Proxy Security Gateway OS (SGOS) 4.1.2.1	<p>A vulnerability has been reported when using 'Deep Content Inspection' because 'CONNECT' rules are not enforced, which could let a remote malicious user bypass connection filters.</p> <p><a href="#">Workaround available</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Blue Coat ProxySG Policy Error Rules Bypass</p> <p><a href="#">CVE-2006-0578</a></p>	<a href="#">7</a>	Security Tracker Alert ID: 1015644, February 17, 2006
BomberClone BomberClone prior to 0.11.6.2; Gentoo Linux	<p>A buffer overflow vulnerability has been reported due to a boundary error when processing error messages, which could let a remote malicious user</p>	<p>BomberClone Error Messages Buffer Overflow</p> <p><a href="#">CVE-2006-0460</a></p>	<a href="#">7</a>	<p>Security Focus, Bugtraq ID: 16697, February 17, 2006</p> <p>Gentoo Linux Security Advisory, GLSA</p>

	<p>execute arbitrary code.</p> <p><a href="#">Gentoo</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>			200602-09, February 16, 2006
<p>BoonEx</p> <p>Barracuda Directory 1.1</p>	<p>HTML injection vulnerabilities have been reported in the 'Add URL' and 'Suggest Category' functionality due to insufficient sanitization of various fields, 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>There is no exploit code required.</p>	<p>Barracuda Directory Multiple HTML Injection</p> <p><a href="#">CVE-2006-0833</a></p>	<a href="#">2.3</a>	Secunia Advisory: SA18965, February 21, 2006
<p>Calacode</p> <p>@Mail 4.3</p>	<p>A vulnerability has been reported due to insufficient sanitization of email messages that contain HTML image tags with 'javascript' URLs that have '&amp;#09;' in the middle, which could let a remote malicious user execute arbitrary JavaScript code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>@Mail HTML Injection</p> <p><a href="#">CVE-2006-0842</a></p>	<a href="#">2.3</a>	Secunia Advisory: SA18874, February 16, 2006
<p>CherryPy</p> <p>CherryPy 2.1, 2.0</p>	<p>A Directory Traversal vulnerability has been reported in the 'staticfilter' functionality due to an input validation error, which could let a remote malicious user obtain sensitive information.</p> <p><a href="#">Updates available</a></p> <p>There is no exploit code required.</p>	<p>CherryPy Directory Traversal</p> <p><a href="#">CVE-2006-0847</a></p>	<a href="#">2.3</a>	Secunia Advisory: SA18944, February 21, 2006
<p>Clever Copy</p> <p>Clever Copy 3.0</p>	<p>An HTML injection vulnerability has been reported in the Private Messages functionality due to insufficient sanitization of the 'Subject' field before storing, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch</p>	<p>Clever Copy Private Message HTML Injection</p> <p><a href="#">CVE-2006-0796</a></p>	<a href="#">2.3</a>	Secunia Advisory: SA18873, February 16, 2006

	<p>available at time of publishing.</p> <p>There is no exploit code required.</p>			
<p>CPG-Nuke</p> <p>CPG Dragonfly Dragonfly CMS 9.0.6 .1</p>	<p>Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'linking.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code.</p> <p>The vulnerability has been fixed in the CVS repository.</p> <p>Vulnerability can be exploited through a web client.</p>	<p>CPG Dragonfly CMS Cross-Site Scripting &amp; SQL Injection</p> <p><a href="#">CVE-2006-0726</a> <a href="#">CVE-2006-0727</a></p>	<p><a href="#">2.3</a> (CVE-2006-0726)</p> <p><a href="#">7</a> (CVE-2006-0727)</p>	<p>Secunia Advisory: SA18919, February 22, 2006</p>
<p>devScripts</p> <p>Admbook 1.2.2</p>	<p>A vulnerability has been reported in the 'content-data.php' file due to insufficient sanitization of the 'X-Forwarded-For' header in the HTTP request, which could let a remote malicious user execute arbitrary PHP 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 script, admbook_122_xpl.pl, has been published.</p>	<p>Admbook Remote Arbitrary PHP Code Execution</p> <p><a href="#">CVE-2006-0852</a></p>	<p><a href="#">7</a></p>	<p>Security Focus, Bugtraq ID: 16753, February 21, 2006</p>
<p>Digital Dominion</p> <p>PHP-Fusion 4.x, 5.x, 6.x</p>	<p>Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'shoutbox_panel.php' due to insufficient sanitization of the 'shout_name' field and in 'comments_include.php' due to insufficient of certain unspecified fields, which could let a remote malicious user execute arbitrary HTML and script code; and an unspecified vulnerability was reported in 'messages.php' due to the way the 'srch_text' parameter is handed.</p>	<p>PHP-Fusion Cross-Site Scripting</p> <p><a href="#">CVE-2006-0593</a></p>	<p><a href="#">2.3</a></p>	<p>Secunia Advisory: SA18949, February 21, 2006</p>

	<p><a href="#">Updates available</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>			
D-Link DWL-G700AP 2.01, DWL-G700AP 2.00	<p>A remote Denial of Service vulnerability has been reported in the 'httpd' service due to a failure to properly handle malformed data.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploit scripts, death_link.c and DWL-G700AP.txt, have been published.</p>	D-Link DWL-G700AP Remote Denial of Service  <a href="#">CVE-2006-0784</a>	<a href="#">2.3</a>	Security Focus, Bugtraq ID: 16690, February 17, 2006
Dovecot Dovecot 1.0.beta2, 1.0	<p>A remote Denial of Service vulnerability has been reported in 'pop3-login' and 'imap-login' due to a double free error when processing certain requests.</p> <p><a href="#">Updates available</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Dovecot Double Free Remote Denial of Service  <a href="#">CVE-2006-0730</a>	<a href="#">2.3</a>	Security Focus, Bugtraq ID: 16672, February 15, 2006
Dreamcost HostAdmin 3.0	<p>A file include vulnerability has been reported in 'index.php' due to insufficient verification of the 'path' parameter, which could let a remote malicious user include arbitrary files.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploit scripts, XOR-HostAdmin.txt and HostAdmin_rm-inc.php, have been published.</p>	DreamCost HostAdmin Remote File Include  <a href="#">CVE-2006-0791</a>	<a href="#">7</a>	XOR Crew Security Advisory, February 11, 2006
E107.org e107 website system 0.7.2	<p>An HTML injection vulnerability has been reported in the Chatbox plugin due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code.</p>	E107 Website System HTML Injection	Not Available	Security Focus, Bugtraq ID: 16719, February 18, 2006

	<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>E-Blah</p> <p>E-Blah Platinum 9.7</p>	<p>An HTML injection vulnerability has been reported in 'Routines.PL' due to insufficient sanitization of user-supplied input before using in dynamically generated content, 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>There is no exploit code required.</p>	<p>E-Blah HTML Injection</p> <p><a href="#">CVE-2006-0829</a></p>	<p><a href="#">2.3</a></p>	<p>Security Focus, Bugtraq ID: 16713, February 17, 2006</p>
<p>EmuLinker</p> <p>EmuLinker prior to 0.99.17</p>	<p>A remote Denial of Service vulnerability has been reported due to a failure to properly handle malformed network packets from other game players.</p> <p><a href="#">Update available</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>EmuLinker Remote Denial of Service</p> <p><a href="#">CVE-2006-0822</a></p>	<p><a href="#">2.3</a></p>	<p>Secunia Advisory: SA18938, February 20, 2006</p>
<p>Ethereal Group</p> <p>Ethereal 0.10-0.10.13, 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</p>	<p>A buffer overflow vulnerability has been reported in the 'dissect_ospf_v3_address_prefix()' function in the OSPF protocol dissector due to a boundary error when converting received binary data to a human readable string, which could let a remote malicious user execute arbitrary code.</p> <p><a href="#">Patch available</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Gentoo</a></p> <p><a href="#">Mandriva</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Avaya</a></p>	<p>Ethereal OSPF Protocol Dissection Buffer Overflow</p> <p><a href="#">CVE-2005-3651</a></p>	<p><a href="#">7</a></p>	<p>iDefense Security Advisory, December 9, 2005</p> <p>Debian Security Advisory DSA 920-1, December 13, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200512-06, December 14, 2005</p> <p>Mandriva Linux Security Advisory MDKSA-2005:227, December 15, 2005</p> <p>Mandriva Linux Security Advisory MDKSA-2006:002, January 3, 2006</p> <p>Fedora Update Notification FEDORA-2005-000, January 5, 2006</p>

	Currently we are not aware of any exploits for this vulnerability.			RedHat Security Advisory, RHSA-2006:0156-6, January 11, 2006  <b>Avaya Security Advisory, ASA-2006-046, February 13, 2006</b>
Ethereal Group  Ethereal 0.9.1-0.10.13.	A remote Denial of Service vulnerability has been reported in the IRC and GTP dissectors when a malicious user submits a specially crafted packet.  <a href="#">Upgrades available</a>  <a href="#">Mandriva</a>  <a href="#">RedHat</a>  <a href="#">Avaya</a>  Currently we are not aware of any exploits for this vulnerability.	Ethereal IRC & GTP Dissectors Remote Denial of Service  <a href="#">CVE-2005-4585</a>	<a href="#">3.3</a>	Ethereal Security Advisory, enpa-sa-00022, December 27, 2005  Mandriva Linux Security Advisory MDKSA-2006:002, January 3, 2006  RedHat Security Advisory, RHSA-2006:0156-6, January 11, 2006  <b>Avaya Security Advisory, ASA-2006-046, February 13, 2006</b>
Francisco Burzi  PHP-Nuke 7.8 & prior	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization the 'Your_Account' module before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.  <a href="#">Updates available</a>  There is no exploit code required; however, Proof of Concept exploit scripts, PHPNuke-Your_Account.txt and phpnuke-sp3x.c, have been published.	PHPNuke SQL Injection  <a href="#">CVE-2006-0679</a>	<a href="#">7</a>	Secunia Advisory: SA18931, February 17, 2006
Gregory DEMAR  Coppermine Photo Gallery 1.4.3 & prior	Several vulnerabilities have been reported: a file include vulnerability was reported in 'include/init.inc.php' due to insufficient verification of the 'lang' parameter, which could let a remote malicious user execute arbitrary PHP code; and a file include vulnerability was reported in 'docs/showdoc.php' due to insufficient verification of the 'f' parameter, which could let a remote malicious user execute arbitrary PHP code.	Coppermine Photo Gallery File Include	Not Available	Security Tracker Alert ID: 1015646, February 18, 2006

	<p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits and an exploit script, <code>cpg_143_incl_xpl</code>, have been published.</p>			
<p>Guestbox</p> <p>Guestbox 0.6</p>	<p>Multiple vulnerabilities have been reported: a vulnerability was reported in the authentication process due to an error, which could let a remote malicious user obtain unauthorized access and post comments; a vulnerability was reported in 'guestbox.php' when posting an entry due to insufficient sanitization of the 'url' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'gblog' file because IP addresses are stored insecurely, which could let a remote malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>Guestbox Vulnerabilities</p>	<p>Not Available</p>	<p>Secunia Advisory: SA18946, February 21, 2006</p>
<p>HTML::BBCode</p> <p>HTML::BBCode 1.04, 1.03</p>	<p>An HTML injection vulnerability has been reported due to insufficient sanitization of the '[url]' and '[img]' BBcode tags before converting to HTML, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p><a href="#">Updates available</a></p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>HTML::BBCode HTML Injection</p>	<p>Not Available</p>	<p>Security Focus, Bugtraq ID: 16680, February 16, 2006</p>
<p>ilch.de</p> <p>ilchClan 1.0.5</p>	<p>Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'pid' parameter due to insufficient sanitization before using in an SQL</p>	<p>ilchClan SQL Injection</p> <p><a href="#">CVE-2006-0850</a> <a href="#">CVE-2006-0851</a></p>	<p><a href="#">Z</a> (CVE-2006-0850)</p> <p><a href="#">Z</a> (CVE-2006-0851)</p>	<p>Security Focus, Bugtraq ID: 16735, February 21, 2006</p>

	<p>query, which could let a remote malicious user execute arbitrary SQL code; and an SQL injection vulnerability was reported in 'login.php' due to insufficient sanitization of the 'login_name' 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 script, ilchclan_poc, has been published.</p>			
<p>InfoVista VistaPortal Standard Edition 2.0</p>	<p>Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in 'PortalSE' due to insufficient sanitization, which could let a remote malicious user obtain sensitive information; and an input validation vulnerability was reported due to the way server field is handled, which could let a remote malicious user obtain sensitive information.</p> <p>The vendor has released a hotfix (IV00038969) to address this issue. Users are advised to contact the vendor for information on obtaining the appropriate updates.</p> <p>Vulnerability may be exploited with a web client.</p>	<p>InfoVista VistaPortal Directory Traversal &amp; Input Validation</p>	<p>Not Available</p>	<p>IRM Security Advisory No. 017, February 17, 2006</p>
<p>Kyocera FS-3830N Printer 0</p>	<p>A vulnerability has been reported due to insufficient authentication before granting access to printer functions, which could let a remote malicious user obtain sensitive information or modify system information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>Kyocera 3830 Printer Unauthorized Access  <a href="#">CVE-2006-0788</a></p>	<p><a href="#">2.3</a></p>	<p>Security Focus, Bugtraq ID: 16685, February 17, 2006</p>

<p>Leif M. Wright Blog 3.5</p>	<p>Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient access restriction to 'txt' files using '.htaccess,' which could let a remote malicious user obtain sensitive information; a vulnerability was reported in the 'blog.cgi' script due to insufficient validation of the password submitted via the cookie when validating administrator access, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported because an administrative user can edit the full path to the 'sendmail' program when modifying the blog, which could let a remote malicious user execute arbitrary shell commands; and an HTML injection vulnerability was reported due to insufficient sanitization of the 'HTTP_REFERER' and 'HTTP_USER_AGENT HTTP' request headers before saving, 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>There is no exploit code required.</p>	<p>Leif M. Wright's Blog Multiple Vulnerabilities</p> <p><a href="#">CVE-2006-0843</a> <a href="#">CVE-2006-0844</a> <a href="#">CVE-2006-0845</a> <a href="#">CVE-2006-0846</a></p>	<p><a href="#">2.3</a> (CVE-2006-0843)</p> <p><a href="#">7</a> (CVE-2006-0844)</p> <p><a href="#">4.2</a> (CVE-2006-0845)</p> <p><a href="#">2.3</a> (CVE-2006-0846)</p>	<p>Secunia Advisory: SA18923, February 17, 2006</p>
<p>Mambo Mambo Open Source 4.5-4.5.3, 4.0.14</p>	<p>An unspecified vulnerability has been reported, which potentially could let a remote malicious user compromise a vulnerable system.</p> <p><a href="#">Patch information</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Mambo Unspecified System Compromise</p>	<p>Not Available</p>	<p>Security Focus, Bugtraq ID: 16775, February 21, 2006</p>
<p>MiniNuke MiniNuke CMS 1.8.2</p>	<p>An SQL injection vulnerability has been reported in 'Pages.ASP' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p>	<p>MiniNuke CMS SQL Injection</p>	<p>Not Available</p>	<p>Security Focus, Bugtraq ID: 16730, February 20, 2006</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 script, MiniNukeCMS.txt, has been published.</p>			
<p>Mozilla Thunderbird 1.5</p>	<p>A remote Denial of Service vulnerability has been reported when handling a specially crafted address book file.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	<p>Mozilla Thunderbird Remote Denial of Service</p> <p><a href="#">CVE-2006-0836</a></p>	<p><a href="#">1.3</a></p>	<p>Security Focus, Bugtraq ID: 16716, February 17, 2006</p>
<p>Mozilla.org Firefox prior to 1.5.0.1</p>	<p>A remote Denial of Service vulnerability has been reported when parsing certain malformed HTML content.</p> <p><a href="#">Updates available</a></p> <p>A Proof of Concept exploit has been published.</p>	<p>Mozilla Firefox HTML Parsing Remote Denial of Service</p>	<p>Not Available</p>	<p>BuHa Security-Advisory #8, February 15, 2006</p>
<p>Mozilla.org Thunderbird 1.0.7 &amp; prior</p>	<p>A script execution vulnerability has been reported when a remote malicious user submits a specially crafted email that contains malicious script code in an IFRAME, which could lead to the execution of arbitrary Javascript 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>Mozilla Thunderbird IFRAME JavaScript Execution</p>	<p>Not Available</p>	<p>Security Focus, Bugtraq ID: 16770, February 22, 2006</p>
<p>Multiple Vendors</p> <p>M. Blom HTML-BBCode 1.04, 1.03; FuzzyMonkey My Blog 1.63</p>	<p>An HTML injection vulnerability has been reported due to insufficient sanitization of BBcode tags before using, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p><a href="#">FuzzyMonkey</a></p> <p><a href="#">M Blum</a></p> <p>There is no exploit code required; however, a Proof of Concept exploit has</p>	<p>My Blog BBCode HTML Injection</p> <p><a href="#">CVE-2006-0735</a></p>	<p><a href="#">2.3</a></p>	<p>Security Focus, Bugtraq ID: 16659, February 15, 2006</p>

	been published.			
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.  <a href="#">Mandriva</a>  <a href="#">Gentoo</a>  <a href="#">SUSE</a>  <a href="#">Conectiva</a>  <a href="#">Mandriva</a>  <a href="#">Avaya</a>  Currently we are not aware of any exploits for this vulnerability.	Ethereal Denial of Service  <a href="#">CVE-2005-3313</a>	<a href="#">3.3</a>	Mandriva Linux Security Advisory, MDKSA-2005:193-1, October 26, 2005  Gentoo Linux Security Advisor, GLSA 200510-25, October 30, 2005  SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005  Conectiva Security Announcement, CLSA-2005:1043, November 8, 2005  Mandriva Linux Security Advisory MDKSA-2006:002, January 3, 2006  <b>Avaya Security Advisory, ASA-2006-046, February 13, 2006</b>
Multiple Vendors  Raven Software Soldier Of Fortune 2 1.0 3, 2 1.0 2; PunkBuster 1.180 & prior	A format string vulnerability has been reported due to insufficient sanitization of user-supplied input before using in a formatted-printing function, which could let a remote malicious user execute arbitrary code.  The vulnerability has reportedly been fixed by the vendor.  Currently we are not aware of any exploits for this vulnerability.	PunkBuster Module Remote Format String  <a href="#">CVE-2006-0771</a>	Not Available	Security Focus, Bugtraq ID: 16703, February 17, 2006
MyBB Group  My BulletinBoard 1.0.3	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported in 'managegroup.php' due to insufficient sanitization of the 'gid' and 'request[ ]' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported in 'managegroup.php' due to insufficient sanitization of the 'gid' parameter before returning to the user in an error message, which could	MyBB Cross-Site Scripting & SQL Injection	Not Available	Secunia Advisory: SA18897, February 17, 2006

	<p>let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported in 'private.php' due to insufficient sanitization of the 'folder[ ]' and 'check[ [ ]' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; an SQL injection vulnerability was reported due to insufficient sanitization of the referrer uid before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and unspecified vulnerabilities were reported when 'register_globals' is enabled.</p> <p><a href="#">Updates available</a></p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>			
<p>MySQL AB MySQL 4.0 .0-4.0.11, 5.0 .0- 5.0.4</p>	<p>A vulnerability has been reported in the 'mysql_install_db' script due to the insecure creation of temporary files, which could let a malicious user obtain unauthorized access.</p> <p><a href="#">Fedora</a></p> <p><a href="#">Debian</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Mandriva</a></p> <p>There is no exploit code required.</p>	<p>MySQL 'mysql_install_db' Insecure Temporary File Creation</p> <p><a href="#">CVE-2005-1636</a></p>	<p><a href="#">4.9</a></p>	<p>Security Focus, 13660, May 17, 2005</p> <p>Fedora Update Notification, FEDORA-2005-557, July 20, 2005</p> <p>Debian Security Advisory, DSA 783-1, August 24, 2005</p> <p>RedHat Security Advisory, RHSA-2005:685-5, October 5, 2005</p> <p><b>Mandriva Linux Security Advisory, MDKSA-2006:045, February 21, 2006</b></p>
<p>PEAR LiveUser 0.16.8 &amp; prior</p>	<p>A file access vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user delete arbitrary files.</p> <p><a href="#">Updates available</a></p> <p>There is no exploit code required.</p>	<p>PEAR LiveUser Unauthorized File Access</p>	<p>Not Available</p>	<p>GulfTech Security Research Team Security Advisory, February 21, 2006</p>

<p>Php Outsourcing</p> <p>Noah's Classifieds 1.3 &amp; prior</p>	<p>Multiple vulnerabilities have been reported: Cross-Site Scripting vulnerabilities were reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported in the Search page due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and file include vulnerabilities were reported which could let a remote malicious user 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 and an exploit script, noah_1.3_rce.php, have been published.</p>	<p>Noah's Classifieds Multiple Vulnerabilities</p>	<p>Not Available</p>	<p>KAPDA Advisory #29, February 22, 2006</p>
<p>PHP-Nuke</p> <p>PHP-Nuke 6.0-7.9</p>	<p>A vulnerability has been reported in the CAPTCHA security feature due to an error, which could let a remote malicious user bypass security features.</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>PHPNuke CAPTCHA Bypass</p> <p><a href="#">CVE-2006-0805</a></p>	<p><a href="#">7</a></p>	<p>waraxe-2006-SA#045, February 18, 2006</p>
<p>PostgreSQL</p> <p>PostgreSQL 8.1.2, 8.1.1, 8.1</p>	<p>Several vulnerabilities have been reported: a vulnerability was reported in the 'SET ROLE' command when previous role settings are restored after an error, which could let a malicious user obtain superuser privileges; and a Denial of Service vulnerability was reported due to an error in the 'SET SESSION AUTHORIZATION' command if compiled with 'Asserts' enabled.</p> <p><a href="#">Updates available</a></p>	<p>PostgreSQL Privilege Escalation &amp; Denial of Service</p> <p><a href="#">CVE-2006-0553</a> <a href="#">CVE-2006-0678</a></p>	<p>Not Available</p>	<p>Secunia Advisory: SA18890, February 15, 2006</p> <p><b>OpenPKG Security Advisory, OpenPKG-SA-2006.004, February 19, 2005</b></p>

	<p><a href="#">OpenPKG</a></p> <p>There is no exploit code required.</p>			
<p>PostNuke</p> <p>PostNuke 0.761 &amp; prior</p>	<p>Multiple vulnerabilities have been reported: a vulnerability was reported in 'pnVarCleanFromInput()' and 'pnAntiCracker()' because it is possible to bypass the HTML tag filter; a Cross-Site Scripting vulnerability was reported in the 'NS-Languages' module due to insufficient sanitization of the 'language' parameter and in 'user.php' due to insufficient sanitization of the 'htmltext' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in 'admin.php' due to an access control error, which could let a remote malicious user obtain unauthorized access; and an SQL injection vulnerability was reported in the 'NS-Languages' module due to insufficient sanitization of the 'language' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p><a href="#">Updates available</a></p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>PostNuke Multiple Vulnerabilities</p> <p><a href="#">CVE-2006-0800</a>  <a href="#">CVE-2006-0801</a>  <a href="#">CVE-2006-0802</a></p>	<p><a href="#">2.3</a> (CVE-2006-0800)</p> <p><a href="#">7</a> (CVE-2006-0801)</p> <p><a href="#">2.3</a> (CVE-2006-0802)</p>	<p>SecurityReason Security Alert 33, February 19, 2006</p>
<p>RR Creates BirthSys 3.1</p>	<p>SQL injection vulnerabilities have been reported in 'show.php' due to insufficient sanitization, 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>BirthSys Multiple SQL Injection</p> <p><a href="#">CVE-2006-0775</a></p>	<p><a href="#">7</a></p>	<p>Security Focus, Bugtraq ID: 16684, February 17, 2006</p>

<p>RunCMS</p> <p>RunCMS 1.2, 1.1 A, 1.1, 1.3.a2, 1.3.a</p>	<p>A Cross-Site Scripting vulnerability has been reported in 'ratefile.php' due to insufficient sanitization of the 'lid' parameter, 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>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>RunCMS Cross-Site Scripting</p>	<p>Not available</p>	<p>Security Focus, Bugtraq ID: 16769, February 22, 2006</p>
<p>RunCMS</p> <p>RunCMS 1.3a3</p>	<p>An SQL injection vulnerability has been reported in '/modules/messages/pmlite.php' due to insufficient sanitization of the 'to_userid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p><b><u>Patch available</u></b></p> <p><b>There is no exploit code required; however, a Proof of Concept exploit script, RUNCMS1.3a-sql.tyxt, has been published.</b></p>	<p>RunCMS SQL Injection</p> <p><a href="#">CVE-2006-0721</a></p>	<p><a href="#">7</a></p>	<p>Secunia Advisory: SA18831, February 14, 2006</p> <p><b>Security Focus, Bugtraq ID: 16652, February 18, 2006</b></p>
<p>SAP</p> <p>Business Connector 4.7, 4.6, Connector Core Fix 7</p>	<p>Several vulnerabilities have been reported: a vulnerability was reported in the Monitoring function due to an unspecified error which could let a remote malicious user read/delete arbitrary files; and a vulnerability was reported due to an unspecified error which could let a remote malicious user conduct spoofing attacks against the SAP BC administrator.</p> <p>The vendor has reportedly released fixes addressing this issue. Users of affected packages should contact the vendor for further information on obtaining fixes.</p> <p>There is no exploit code required.</p>	<p>SAP Business Connector Arbitrary File Access &amp; Spoofing</p> <p><a href="#">CVE-2006-0731</a> <a href="#">CVE-2006-0732</a></p>	<p><a href="#">2.6</a> (CVE-2006-0731)</p> <p><a href="#">4.7</a> (CVE-2006-0732)</p>	<p>Security Tracker Alert ID, 1015639, February 16, 2006</p>

<p>Snort Project</p> <p>Snort 2.4.3</p>	<p>A vulnerability has been reported in the Frag3 preprocessor due to a failure to properly analyze certain packets, which could let a remote malicious user bypass intrusion detection.</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>Snort Frag3 Processor Intrusion Detection Bypass</p> <p><a href="#">CVE-2006-0839</a></p>	<p><a href="#">2.3</a></p>	<p>Security Focus, Bugtraq ID: 16705, February 17, 2006</p>
<p>SquirrelMail Development Team</p> <p>SquirrelMail 1.4.5 &amp; prior</p>	<p>Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'webmail.php' due to insufficient sanitization of the 'right_main' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input passed to comments in styles before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'sqimap_mailbox_select mailbox' parameter due to insufficient sanitization before using in an IMAP query, which could let a remote malicious user inject arbitrary IMAP commands.</p> <p>The vulnerabilities have been fixed in the CVS repository and fixes will be included in the upcoming 1.4.6 version.</p> <p>There is no exploit code required.</p>	<p>SquirrelMail Multiple Cross-Site Scripting &amp; IMAP Injection</p> <p><a href="#">CVE-2006-0188</a>  <a href="#">CVE-2006-0195</a>  <a href="#">CVE-2006-0377</a></p>	<p>Not Available</p>	<p>Secunia Advisory: SA18985, February 22, 2006</p>
<p>Squishdot</p> <p>Squishdot 1.5</p>	<p>A vulnerability has been reported in the 'mail_html' template due to insufficient sanitization before using to construct email messages, which could let a remote malicious user bypass security restrictions.</p> <p><a href="#">Patch available</a></p>	<p>Squishdot Mail Header Injection</p> <p><a href="#">CVE-2006-0712</a></p>	<p><a href="#">2.3</a></p>	<p>Secunia Advisory: SA18868, February 17, 2006</p>

	There is no exploit code required.			
Teca Scripts Guestex 1.0	<p>Several input validation vulnerabilities have been reported: a vulnerability was reported in 'guestex.pl' due to insufficient sanitization of the 'mail' parameter before passing to sendmail as an argument, which could let a remote malicious user execute arbitrary shell commands; and a vulnerability was reported due to insufficient sanitization of the 'url' parameter before returning to the user, 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>There is no exploit code required.</p>	<p>Teca Scripts Guestex Input Validation</p> <p><a href="#">CVE-2006-0776</a> <a href="#">CVE-2006-0777</a></p>	<p><a href="#">2.3</a> (CVE-2006-0776)</p> <p><a href="#">7</a> (CVE-2006-0777)</p>	<p>Secunia Advisory: SA18927, February 17, 2006</p>
Teca Scripts Quirex 2.0.2 & prior	<p>A vulnerability has been reported in 'convert.cgi' due to insufficient sanitization of the 'quiz_head,' 'quiz_foot,' and 'template' parameters before using to display files, which could let a remote malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>Teca Scripts Quirex Information Disclosure</p> <p><a href="#">CVE-2006-0795</a></p>	<p><a href="#">2.3</a></p>	<p>Security Focus, Bugtraq ID: 16709, February 17, 2006</p>
Teca Scripts Teca Diary Personal Edition 1.0	<p>An SQL injection vulnerability has been reported in 'functions.php' due to insufficient sanitization of the 'yy,' 'mm,' and 'dd' 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.</p>	<p>Teca Diary Personal Edition SQL Injection</p> <p><a href="#">CVE-2006-0729</a></p>	<p><a href="#">7</a></p>	<p>Secunia Advisory: SA18876, February 17, 2006</p>
V-webmail V-webmail	<p>Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was</p>	<p>V-webmail Cross-Site</p>	<p><a href="#">2.3</a> (CVE-2006-0792)</p>	<p>Secunia Advisory: SA18776, February 17, 2006</p>

1.6.2	<p>reported in the 'newid' parameter due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in 'frameset.php' due to insufficient verification of the 'rframe' parameter, which could let a remote malicious user conduct phishing attacks; and a vulnerability was reported when the 'help.php' id accessed with invalid parameters, which could let a remote malicious user obtain sensitive information.</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>Scripting &amp; Information Disclosure</p> <p><a href="#">CVE-2006-0792</a> <a href="#">CVE-2006-0793</a> <a href="#">CVE-2006-0794</a></p>	<p><a href="#">2.3</a> (CVE-2006-0793)</p> <p><a href="#">2.3</a> (CVE-2006-0794)</p>	
webSPELL webSPELL 4.01.00 & prior	<p>An SQL injection vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'title_op' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p><a href="#">Updates available</a></p> <p>There is no exploit code required.</p>	<p>WebSPELL SQL Injection</p> <p><a href="#">CVE-2006-0728</a></p>	<p><a href="#">7</a></p>	<p>Security Focus, Bugtraq ID: 16673, February 15, 2006</p>
Wimpy Wimpy MP3 Player 5	<p>A vulnerability has been reported in 'wimpy_trackplays.php' due to insufficient authentication, which could let a remote malicious user modify certain data.</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>Wimpy MP3 Player Text File Overwrite</p> <p><a href="#">CVE-2006-0787</a></p>	<p><a href="#">3.7</a></p>	<p>Security Focus, Bugtraq ID: 16696, February 17, 2006</p>
Xerox WorkCentre Pro 275, 265,	<p>Multiple vulnerabilities have been reported: a vulnerability was reported in the authentication</p>	<p>Xerox ESS/ Network Controller and</p>	<p><a href="#">7</a> (CVE-2006-0825)</p> <p><a href="#">2.3</a></p>	<p>XEROX Security Bulletin, XRX06-001, February 20, 2006</p>

255, 245, 238, 232, WorkCentre 275, 265, 255, 245, 238, 232	<p>process due to unspecified errors, which could let a remote malicious user obtain unauthorized access; a remote Denial of Service vulnerability was reported when processing Postscript requests; an HTML injection vulnerability was reported due to insufficient sanitization of unspecified input passed to certain web pages, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported due to unspecified errors which could reduce the effectiveness of certain security features.</p> <p><a href="#">Update information</a></p> <p>There is no exploit code required.</p>	<p>MicroServer Vulnerabilities</p> <p><a href="#">CVE-2006-0825</a>  <a href="#">CVE-2006-0826</a>  <a href="#">CVE-2006-0827</a>  <a href="#">CVE-2006-0828</a></p>	<p>(CVE-2006-0826)</p> <p><a href="#">2.3</a> (CVE-2006-0827)</p> <p><a href="#">2.3</a> (CVE-2006-0828)</p>	
Xpdf Xpdf 3.01	<p>A heap-based buffer overflow vulnerability has been reported when handling PDF splash images with overly large dimensions, which could let a remote malicious user execute arbitrary code.</p> <p><a href="#">Gentoo</a></p> <p><a href="#">Fedora</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">RedHat</a></p> <p><a href="#">Ubuntu</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Debian</a></p> <p><a href="#">Slackware</a></p> <p><a href="#">Slackware</a></p> <p><a href="#">Gentoo</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Xpdf PDF Splash Remote Buffer Overflow</p> <p><a href="#">CVE-2006-0301</a></p>	<p><a href="#">7</a></p>	<p>Secunia Advisory: SA18677, February 1, 2006</p> <p>Gentoo Linux Security Advisories, GLSA 200602-04 &amp; GLSA 200602-05, February 12, 2006</p> <p>Fedora Update Notifications, FEDORA-2006-103, FEDORA-2006-104, &amp; FEDORA-2006-105, February 10, 2006</p> <p>RedHat Security Advisories, RHSA-2006:0201-3 &amp; RHSA-2006:0206-3, February 13, 2006</p> <p>Ubuntu Security Notice, USN-249-1, February 13, 2006</p> <p>Debian Security Advisories, DSA-971-1, DSA-972-1 &amp; DSA-974-1, February 14 &amp; 15, 2006</p> <p><b>Slackware Security Advisories, SSA:2006-045-04 &amp; SSA:2006-045-09, February 14, 2006</b></p> <p><b>Gentoo Linux Security Advisory, GLSA</b></p>

200602-12, February  
21, 2006

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

## Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- [hcidump Bluetooth L2CAP Remote Denial of Service](#): Ubuntu has released an update for the Denial of Service vulnerability in the L2CAP (Logical Link Control and Adaptation Layer Protocol) layer.
- [Mobile Security: Another Hole To Plug](#): Securing devices are moving up the priority list as companies grant more network and application access via handheld devices such as smart phones. Mobile devices are vulnerable to attacks because users usually aren't behind a firewall. Many smart phones and PDAs now come standard with advanced functions, including Wi-Fi, Bluetooth, and Web-browsing capabilities, which make them more vulnerable.
- [Mobile virus growth outpaces PC malware](#): According to security software vendor McAfee, the number of mobile viruses is climbing faster than PC viruses. Data on virus numbers since 2004 was compared to the number of PC viruses since 1990 and the results show that mobile malware numbers are rising faster than for PCs. So far over 200 mobile viruses have been detected in the wild.
- [Firms urged to tackle Wi-Fi hotspot risks](#): According to a new report compiled by law firm Charles Russell in association with managed Wisp iBahn, firms need to do more to ensure the security of mobile devices used by staff in Wi-Fi hotspots provided by wireless internet service providers (Wisps) or other third parties. Failure to do so could result in legal problems if, for example, data is stolen.

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

## General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- [Public Exploit Code for a Vulnerability in Apple Safari Browser](#): US-CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.
- [Public Exploit Code for Buffer Overflow Vulnerability in Microsoft Windows Media Player Plug-in for Non-IE Browsers](#): US-CERT is aware of publicly available exploit code for a buffer overflow vulnerability in Windows Media Player plug-in for browsers other than Internet Explorer (IE).
- [Public Exploit Code for Buffer Overflow Vulnerability in Microsoft Windows Media Player](#): US-CERT is aware of publicly available exploit code for a buffer overflow vulnerability in Windows Media Player. The vulnerability exists because Windows Media Player fails to properly validate bitmap image files.
- [Cybercrime is an organized and sophisticated business](#): In a town hall meeting held at the 2006 RSA Security Conference by Business Software Alliance (BSA), top law enforcement officials from the United States and Europe said that combating cybercrime requires industry coordination with law enforcement officials on both sides of the Atlantic.
- [First Mac OS virus](#): The first worm, OSX.Leap.A, targeting Apple Computer's Mac OS X operating system has surfaced. This could be an indication that hackers, who have targeted the Windows PC market, are expanding their attacks. The worm is designed to spread over iChat.
- [More Than Half Receive At Least One Phish Daily](#): According to a survey conducted by Sophos of 600 business users, 58 percent reported seeing one or more phishing mails in their inboxes daily. More than 1 in 5 (22 percent) receive five or more each day.
- [Three Out Of Four Say Business Security Has Improved](#): According to a survey conducted by Forsythe Technology, Inc., nearly 30% of IT security pros indicate they have little or no confidence that their companies detected all data security breaches last year. In addition, about 26% of survey respondents rated their current IT environments as more vulnerable than a year ago. Many of the survey respondents blamed increased security vulnerability on organizational changes and "people issues," including mergers and acquisitions and outsourcing.

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

## Viruses/Trojans

### Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected),

common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
3	Mytob-GH	Win32 Worm	Stable	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.
4	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.
5	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
6	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
7	Sober-Z	Win32 Worm	Stable	December 2005	This worm travels as an email attachment, forging the senders address, harvesting addresses from infected machines, and using its own mail engine. It further download code from the internet, installs into the registry, and reduces overall system security.
8	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System%

					directory with randomly generated file names.
9	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.
10	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.

Table updated February 20, 2006

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

Last updated February 23, 2006



PRINTABLE VERSION