US-CERT National Cyber Alert System

SB04-287-Summary of Security Items from October 6 through October 12, 2004

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

Bugs, Holes, & Patches

- Windows Operating Systems
  - AtHoc Toolbar Remote Code Execution Vulnerability
  - Business Objects Crystal Reports Buffer Overflow JPEG Processing
  - IceWarp Web Mail Cross-Site Scripting Vulnerabilities
  - **IPSwitch WhatsUp Gold Remote Buffer Overflow (Updated)**
  - Jera Technology Flash Messaging Denial of Service
  - Microsoft ASP.NET Canonicalization
  - Microsoft Compressed (zipped) Folders Remote Code Execution
  - Microsoft Excel Remote Code Execution
  - Microsoft Internet Explorer Security Update
  - Microsoft Internet Explorer XML Documents Remote Access
  - **Microsoft JPEG Processing Buffer Overflow (Updated)**
  - Microsoft NetDDE Remote Code Execution
  - Microsoft NNTP Remote Code Execution
  - Microsoft RPC Runtime Library Information Disclosure & Denial of Service
  - Microsoft SMTP Remote Code Execution
  - Microsoft WebDav XML Message Handler Denial of Service
  - Microsoft Windows Security Update
  - Microsoft Windows Shell Remote Code Execution
  - Microsoft Word Buffer Overflow
  - Monolith Games Buffer Overflow
  - Robert K Jung unarj Input Validation
  - TriDComm FTP Server Directory Traversal
- UNIX / Linux Operating Systems
  - Cyrus SASL Buffer Overflow & Input Validation
  - **Charles Cazabon Getmail Privilege Escalation (Updated)**
  - **CVS Undocumented Flag Information Disclosure (Updated)**
  - **CVS Multiple Vulnerabilities (Updated)**
  - Debian GNU/Linux Telnetd Invalid Memory Handling
  - **FreeRADIUS Access-Request Denial of Service (Updated)**
  - **GNU GetText Insecure Temporary File Creation (Updated)**
  - INCOGEN, Inc. Bugport File Attachment
  - Jem Berkes Renattach '--pipe' Input Validation
  - **Multiple Vendor Apache mod_dav Remote Denial of Service (Updated)**
  - **Multiple Vendor KDE Insecure Temporary Directory Symlink (Updated)**
  - Multiple Vendor CUPS Error_Log Password Disclosure
  - **Multiple Vendor CUPS Browsing Denial of Service (Updated)**
  - **Multiple Vendor IMLib/IMLib2 Multiple BMP Image (Updated)**
  - **Multiple Vendor QT Image File Buffer Overflows (Updated)**
  - **Multiple Vendor Konqueror Frame Injection (Updated)**
  - **Multiple Vendor LinuxPrinting.org Foomatic-Filter Arbitrary Code Execution (Updated)**
  - **Multiple Vendor Samba Remote Arbitrary File Access (Updated)**
  - Nathaniel Bray Yeemp File Transfer Public Key Verification Bypass
  - Squid Remote Denial of Service
  - **Ulrich Callmeier Net-acct Insecure Temporary File (Updated)**
  - **XFree86 XDM RequestPort False Sense of Security (Updated)**
  - **Xine-lib Multiple Buffer Overflows (Updated)**
- Multiple Operating Systems
  - CubeCart Input Validation
  - CJOverkill Cross-Site Scripting
  - Content Management System DCP-Portal Multiple Cross-Site Scripting Vulnerabilities
  - Duware DUclassified Input Validation Vulnerabilities
  - Duware DUclassmate Password Change Request
  - Duware DUforum Input Validation Vulnerabilities
  - IBM DB2 Multiple Buffer Overflows
  - **Icecast Server HTTP Header Buffer Overflow (Updated)**
  - Invision Power Board Referer Cross-Site Scripting
  - Macromedia ColdFusion Default Configuration Elevated Privileges
  - Macromedia ColdFusion MX Remote File Content Disclosure
  - Matthew Phillips Sticker Unauthorized Secure Message
  - **Mozilla / Firefox Certificate Store Corruption Vulnerability (Updated)**
  - **Mozilla / Mozilla Firefox "onunload" SSL Certificate Spoofing (Updated)**
  - **Netscape/Mozilla SOAPParameter Constructor Integer Overflow Vulnerability (Updated)**
  - Mozilla Firefox DATA URI File Deletion
  - **Mozilla/Firefox/Thunderbird Multiple Vulnerabilities (Updated)**
  - **Mozilla Multiple Remote Vulnerabilities (Updated)**
  - **Multiple Vendor AJ-Fork Insecure Default Permissions (Updated)**
  - Multiple Vendor PHP PHP_Variables Remote Memory Disclosure
  - Multiple Vendor Jetty Directory Traversal
  - MySQL MaxDB WebDBM Server Name Denial of Service
  - MySQL Security Restriction Bypass & Remote Denial of Service
  - **PNG Development Group Multiple Vulnerabilities in libpng (Updated)**
  - Real Networks Helix Universal Server Remote Denial of Service
  - The BNG Project BNC Buffer Overflow
  - Turbo Traffic Trader Nitro Cross-Site Scripting & SQL Injection
  - **Wordpress Multiple Cross-Site Scripting (Updated)**

  - Yves Goergen BlackBoard Internet Newsboard System Remote File Include
  - Zanfi CMS Multiple Vulnerabilities
- Recent Exploit Scripts/Techniques
- Trends
- Viruses/Trojans

Bugs, Holes, & Patches

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

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

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

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

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
AtHoc AtHoc Toolbar	Two vulnerabilities were reported in the AtHoc Toolbar plug-in for Microsoft Internet Explorer. Due to a buffer overflow and a format string flaw in the toolbar software, a remote user can execute arbitrary code on the target user's system with the privileges of the target user. Upgrade available at: www.athoc.com/site/products/toolbar.asp We are not aware of any exploits for this vulnerability.	AtHoc Toolbar Remote Code Execution	High	SecurityTracker Alert ID: 1011554, October 6, 2004
Business Objects Crystal Reports 9, 10 Crystal Enterprise 9, 10	A buffer overflow vulnerability exists in certain Crystal products when processing Joint Photographic Experts Group (JPEG) image files, which could allow remote code execution. The vulnerability is due to a Microsoft component (Gdiplus.dll) included with certain versions of Crystal Reports and Crystal Enterprise. Updates available at: http://support.businessobjects.com/library/kbase/articles/c2016358.asp We are not aware of any exploits for this vulnerability.	Business Objects Crystal Reports Buffer Overflow JPEG Processing	High	Business Objects, October 2004
IceWarp IceWarp Web Mail prior to 5.3.0	Vulnerabilities exist in IceWarp Web Mail, which can be exploited by malicious people to conduct cross-site scripting attacks. These vulnerabilities are due to input validation errors in 'view.html.' Update to version 5.3.0: http://www.icewarp.com/Download/ We are not aware of any exploits for this vulnerability.	IceWarp Web Mail Cross-Site Scripting Vulnerabilities	High	Secunia Advisory ID SA12789, October 12, 2004
Ipswitch WhatsUp Gold 7.0 4, 7.0 3, 7.0, 8.0 3, 8.0 1, 8.0	A buffer overflow vulnerably exists in the '_maincfgret.cgi' script due to a failure to validate user-supplied string lengths, which could let a remote malicious user execute arbitrary code. Upgrades available at: ftp://ftp.ipswitch.com/Ipswitch/Product_Support/WhatsUp/wug803HF1.exe **Exploit scripts have been published.**	WhatsUp Gold Remote Buffer Overflow CVE Name: CAN-2004-0798	High	iDEFENSE Security Advisory, August 25, 2004 **SecurityFocus, October 6, 2004**
Jera Technology Flash Messaging 5.2.0g (rev 1.1.2) and prior	A Denial of Service vulnerability exists due to input validation errors in the network data exchanged between server and clients. Also, commands, such as shutdown, from the server to users can be ignored. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Jera Technology Flash Messaging Denial of Service	Low	Bugtraq, October 7, 2004
Microsoft ASP.NET 1.x	A vulnerability exists which can be exploited by malicious people to bypass certain security restrictions. The vulnerability is caused due to a canonicalization error within the .NET authentication schema. Apply ASP.NET ValidatePath module: http://www.microsoft.com/downloads/details.aspx?FamilyId=DA77B852-DFA0-4631-AAF9-8BCC6C743026 A Proof of Concept exploit has been published.	Microsoft ASP.NET Canonicalization CVE Name: CAN-2004-0847	Medium	Microsoft, October 7, 2004
Microsoft Windows XP Home	A remote code execution vulnerability exists in Compressed (zipped) Folders because of an unchecked buffer in the way that it handles specially crafted compressed files. A malicious user could exploit the vulnerability by constructing a	Microsoft Compressed (zipped) Folders	High	Microsoft Security Bulletin MS04-034,

Edition, XP Professional, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition	malicious compressed file that could potentially allow remote code execution if a user visited a malicious web site. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-034.mspx We are not aware of any exploits for this vulnerability.	Remote Code Execution CVE Name: CAN-2004-0575		October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004
Microsoft Office 2000, Excel 2000, Office XP, Excel 2002, Office 2001 for Macintosh, Office v. X for Macintosh	A remote code execution vulnerability exists in Excel. If a user is logged on with administrative privileges, a malicious user who successfully exploited this vulnerability could take complete control of the affected system. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-033.mspx We are not aware of any exploits for this vulnerability.	Microsoft Excel Remote Code Execution CVE Name: CAN-2004-0846	High	Microsoft Security Bulletin MS04-033, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004
Microsoft Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 6.0 for Windows Server 2003, Internet Explorer 6.0 for Windows XP Service Pack 2, Windows 98, Windows 98 SE, Windows ME, Internet Explorer 5.5	Multiple vulnerabilities are corrected with Microsoft Security Update MS04-038. These vulnerabilities include: Cascading Style Sheets (CSS) Heap Memory Corruption Vulnerability; Similar Method Name Redirection Cross Domain Vulnerability; Install Engine Vulnerability; Drag and Drop Vulnerability; Address Bar Spoofing on Double Byte Character Set Locale Vulnerability; Plug-in Navigation Address Bar Spoofing Vulnerability; Script in Image Tag File Download Vulnerability; SSL Caching Vulnerability. These vulnerabilities could allow remote code execution. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-038.mspx We are not aware of any exploits for these vulnerabilities.	Microsoft Internet Explorer Security Update CVE Names: CAN-2004-0842 CAN-2004-0727 CAN-2004-0216 CAN-2004-0839 CAN-2004-0844 CAN-2004-0843 CAN-2004-0841 CAN-2004-0845	High	Microsoft Security Bulletin MS04-038, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004
Microsoft Internet Explorer 6.0, SP1&SP2	A vulnerability was reported in Microsoft Internet Explorer, which could allow a remote malicious user to access XML documents that are accessible to the target user. A remote user can create HTML code that, when loaded by the target user, will retrieve XML data from arbitrary servers and forward that information to the remote user. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer XML Documents Remote Access	Medium	SecurityTracker Alert ID: 1011563, October 7, 2004
Microsoft Microsoft .NET Framework 1.x, Digital Image Pro 7.x, 9.x, Digital Image Suite 9.x, Frontpage 2002, Greetings 2002, Internet Explorer 6, Office 2003 Professional Edition, 2003 Small Business Edition, 2003 Standard Edition, 2003 Student and Teacher Edition, Office XP, Outlook 2002, 2003, Picture It! 2002, 7.x, 9.x, PowerPoint 2002, Producer for Microsoft Office PowerPoint 2003, Project 2002, 2003, Publisher 2002, Visio 2002, 2003, Visual Studio .NET 2002, 2003, Word 2002; Avaya DefinityOne Media Servers, IP600 Media Servers, S3400 Modular Messaging, S8100 Media Servers	A buffer overflow vulnerability exists in the processing of JPEG image formats, which could let a remote malicious user execute arbitrary code. Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx **Another exploit script has been published.**	Microsoft JPEG Processing Buffer Overflow CVE Name: CAN-2004-0200	High	Microsoft Security Bulletin, MS04-028, September 14, 2004 US-CERT Vulnerability Note VU#297462, September 14, 2004 Technical Cyber Security Alert TA04-260A, September 16, 2004 SecurityFocus, September 17, 2004 SecurityFocus, September 28, 2004 **Packet Storm, October 7, 2004.**
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows	A remote code execution vulnerability exists in the NetDDE services because of an unchecked buffer. A malicious user who successfully exploited this vulnerability could take complete control of an affected system. However, the NetDDE services are not started by default and would have to be manually started for an attacker to attempt to remotely exploit this vulnerability. This vulnerability could also be used to attempt to perform a local elevation of privilege or remote Denial of Service. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-031.mspx We are not aware of any exploits for these vulnerabilities.	Microsoft NetDDE Remote Code Execution CVE Name: CAN-2004-0206	High	Microsoft Security Bulletin MS04-031, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004

Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Windows 98, Windows 98 SE, Windows ME				
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Server, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Exchange 2000 Server, Exchange Server 2003	A remote code execution vulnerability exists within the Network News Transfer Protocol (NNTP) component of the affected operating systems, which could let a remote malicious user execute arbitrary code. This vulnerability could potentially affect systems that do not use NNTP. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-036.mspx We are not aware of any exploits for this vulnerability.	Microsoft NNTP Remote Code Execution CVE Name: CAN-2004-0574	High	Microsoft Security Bulletin MS04-036, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition	An information disclosure and Denial of Service vulnerability exists when the RPC Runtime Library processes specially crafted messages. A malicious user who successfully exploited this vulnerability could potentially read portions of active memory or cause the affected system to stop responding. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-029.mspx We are not aware of any exploits for these vulnerabilities.	Microsoft RPC Runtime Library Information Disclosure & Denial of Service CVE Name: CAN-2004-0569	Low	Microsoft Security Bulletin MS04-029, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004
Microsoft Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Exchange Server 2003	A remote code execution vulnerability exists in the Windows Server 2003 SMTP component because of the way that it handles Domain Name System (DNS) lookups. A malicious user could exploit the vulnerability by causing the server to process a particular DNS response that could potentially allow remote code execution. The vulnerability also exists in the Microsoft Exchange Server 2003 Routing Engine component when installed on Microsoft Windows 2000 Service Pack 3 or on Microsoft Windows 2000 Service Pack 4. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx We are not aware of any exploits for this vulnerability.	Microsoft SMTP Remote Code Execution CVE Name: CAN-2004-0840	High	Microsoft Security Bulletin MS04-035, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004
Microsoft Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Internet Information Services 5.0, Internet Information Services 5.1, Internet Information Services 6.0	A Denial of Service vulnerability exists that could allow a malicious user to send a specially crafted WebDAV request to a server that is running IIS and WebDAV. A malicious user could cause WebDAV to consume all available memory and CPU time on an affected server. The IIS service would have to be restarted to restore functionality. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-030.mspx We are not aware of any exploits for these vulnerabilities.	Microsoft WebDav XML Message Handler Denial of Service CVE Name: CAN-2004-0718	Low	Microsoft Security Bulletin MS04-030, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows	Multiple vulnerabilities are corrected with Microsoft Security Update MS04-032. These vulnerabilities include: Window Management Vulnerability, Virtual DOS Machine Vulnerability, Graphics Rendering Engine Vulnerability, Windows Kernel Vulnerability. These vulnerabilities could permit elevation of privilege, remote code execution, and Denial of Service. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-032.mspx We are not aware of any exploits for these vulnerabilities.	Microsoft Windows Security Update CVE Name: CAN-2004-0207 CAN-2004-0208 CAN-2004-0209 CAN-2004-0211	High	Microsoft Security Bulletin MS04-032, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004

Server 2003, Datacenter Edition, Windows Server 2003, Enterprise Edition, Windows Server 2003, Standard Edition, Windows Server 2003, Web Edition, Windows 98, Windows 98 SE, Windows ME				
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Server, Windows 2000 Professional, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Windows Server 2003 Datacenter Edition, Windows 98, Windows 98 SE, Windows ME	A Shell vulnerability and Program Group vulnerability exists in Microsoft Windows. These vulnerabilities could allow remote code execution. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx We are not aware of any exploits for these vulnerabilities.	Microsoft Windows Shell Remote Code Execution CVE Names: CAN-2004-0214 CAN-2004-0572	High	Microsoft Security Bulletin MS04-037, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004
Microsoft Office 2000, XP, Word 2000, 2002	A vulnerability exists in Microsoft Word, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially execute arbitrary code. The vulnerability is caused due to an input validation error within the parsing of document files and may lead to a stack-based buffer overflow. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Microsoft Word Buffer Overflow	Low/High (High if arbitrary code can be executed)	SecurityFocus, Bugtraq ID 11350, October 7, 2004
Monolith Alien versus Predator 2 v1.0.9.6; Blood 2 v2.1; No one lives forever, v1.004; Shogo, v2.2	A buffer overflow vulnerability exists in multiple Monolith games, which can be exploited by malicious people to cause a DoS (Denial of Service) and remote code execution. The vulnerability is caused due to a boundary error within the handling of secure Gamespy queries server. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Monolith Games Buffer Overflow	Low/High (High if arbitrary code can be executed)	Secunia Advisory SA12776, October 10, 2004
Robert K Jung unarj 2.x	An input validation vulnerability was reported in unarj, which could permit a remote user to create a malicious archive that, when expanded by a target user, will write or overwrite arbitrary files on the target user's system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	unarj Input Validation	High	SecurityTracker Alert ID: 1011610, October 11, 2004
TriDComm TriDComm FTP Server 1.3 and prior	A vulnerability exists due to an input validation error which can be exploited by malicious users to access arbitrary files on a the integrated FTP server. No workaround or patch available at time of publishing. An exploit script has been published.	TriDComm FTP Server Directory Traversal	Medium	Secunia Advisory SA 12755, October 7, 2004

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Carnegie Mellon University Cyrus SASL 1.5.24, 1.5.27, 1.5.28, 2.1.9-2.1.18	Several vulnerabilities exist: a buffer overflow vulnerability exists in 'digestmda5.c,' which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'SASL_PATH' environment variable, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-05.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-546.html Trustix: ftp://ftp.trustix.org/pub/trustix/updates/	Cyrus SASL Buffer Overflow & Input Validation CVE Name: CAN-2004-0884	High	SecurityTracker Alert ID: 1011568, October 7, 2004

	We are not aware of any exploits for this vulnerability.			
Charles Cazabon getmail 4.0.0b10, 4.0-4.0.13, 4.1-4.1.5; Gentoo Linux 1.4	A vulnerability exists due to insufficient validation of symbolic links when creating users' mail boxes and subdirectories, which could let a malicious user obtain elevated privileges. Upgrades available at: http://www.qcc.ca/~charlesc/software/getmail-4/old-versions/getmail-4.2.0.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-32.xml Debian: http://security.debian.org/pool/updates/main/g/getmail/ **Slackware: ftp://ftp.slackware.com/pub/slackware/** There is no exploit code required.	Getmail Privilege Escalation	Medium	Secunia Advisory, SA12594, September 20, 2004 Debian Security Advisory, DSA 553-1, September 27, 2004 **Slackware Security Advisory, SSA:2004-278-01, October 4, 2004**
Concurrent Versions Systems (CVS) 1.11	A vulnerability exists in Concurrent Versions System (CVS) in which a malicious user can exploit to determine the existence and permissions of arbitrary files and directories. The problem is caused due to an undocumented switch to the "history" command implemented in "src/history.c". Using the "-X" switch and supplying an arbitrary filename, CVS will try to access the specified file and returns various information depending on whether the file exists and can be accessed. Upgrade to version 1.11.17 or 1.12.9 available at: https://www.cvshome.org/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:14/cvs.patch **Fedora Legacy: http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit has been published.	CVS Undocumented Flag Information Disclosure CVE Name: CAN-2004-0778	Low	iDEFENSE Security Advisory 08.16.04 FreeBSD Security Advisory, FreeBSD-SA-04:14, September 20, 2004 **Fedora Legacy Update Advisory, FLSA:1735, October 7, 2004**
CVS Caldera Conectiva Debian Fedora Gentoo Immunix Mandrake OpenBSD OpenPKG RedHat SGI Slackware SuSE CVS 1.10.7, 1.10.8, 1.11-1.11.6, 1.11.10, 1.11.11, 1.11.14-1.11.16, 1.12.1, 1.12.2, 1.12.5, 1.12.7, 1.12.8; Gentoo Linux 1.4; OpenBSD – current, 3.4, 3.5; OpenPKG Current, 1.3, 2.0	Multiple vulnerabilities exist: a null-termination vulnerability exists regarding ‘Entry’ lines that was introduced by a previous CVS security patch, which could let a remote malicious user execute arbitrary code; a ‘double free’ vulnerability exists in the ‘Arguments ‘command, which could let a remote malicious user execute arbitrary code; a format string vulnerability exists in the processing of the CVS wrapper file, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability exists in the handling of the ‘Max-dotdot’ CVS protocol command, which could let a remote malicious user cause a Denial of Service; a vulnerability exists in the ‘serve_notify()’ function when handling empty data lines, which could let a remote malicious user execute arbitrary code; several errors exist when reading configuration files containing empty lines from CVSROOT, which could let a remote malicious user cause a Denial of Service; and various integer multiplication overflow vulnerabilities exist, which could let a remote malicious user execute arbitrary code. CVS: https://ccvs.cvshome.org/files/documents/19/194/cvs-1.11.17.tar.gz Debian:http://security.debian.org/pool/updates/main/c/cvs/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1 Gentoo: http://security.gentoo.org/glsa/glsa-200406-06.xml Mandrake: http://www.mandrakesoft.com/security/advisories OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ OpenPKG: ftp://ftp.openpkg.org/release RedHat: http://rhn.redhat.com/errata/RHSA-2004-233.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ SuSE: ftp://ftp.suse.com/pub/suse/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:14/cvs.patch **Fedora Legacy: http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit script has been published.	CVS Multiple Vulnerabilities CVE Names: CAN-2004-0418, CAN-2004-0417, CAN-2004-0416, CAN-2004-0414	Low/ High (Low if a DoS; and High if arbitrary code can be executed)	Debian Security Advisories, DSA 517-1 & 519-1, June 10 & 15, 2004 Fedora Update Notifications, FEDORA-2004-169 & 170, June 11, 2004 Gentoo Linux Security Advisory, GLSA 200406-06, June 10, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:058, June 9, 2004 OpenPKG Security Advisory , OpenPKG-SA-2004.027, June 11, 2004 RedHat Security Advisory, RHSA-2004:233-07, June 9, 2004 SGI Security Advisories, 20040604-01-U & 20040605-01-U, June 21, 2004 SUSE Security Announcement, SuSE-SA:2004:015, June 9, 2004 FreeBSD Security Advisory, FreeBSD-SA-04:14, September 20, 2004 **Fedora Legacy**

				Update Advisory, FLSA:1735, October 7, 2004
Debian telnetd 0.17 -25, 0.17 -18	A vulnerability exists due to a failure to ensure that memory buffers are properly allocated and deallocated, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/ We are not aware of any exploits for this vulnerability.	Debian GNU/Linux Telnetd Invalid Memory Handling CVE Name: CAN-2004-0911	Low/High (High if arbitrary code can be executed)	Debian Security Advisory, DSA 556-1, October 3, 2004
FreeRADIUS Server Project FreeRADIUS 0.2-0.5, 0.8, 0.8.1, 0.9-0.9.3. 1.0	A remote Denial of Service vulnerability exists in 'radius.c' and 'eap_tls.c' due to a failure to handle malformed packets. Upgrades available at: ftp://ftp.freeradius.org/pub/radius/freeradius-1.0.1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-29.xml There is no exploit code required.	FreeRADIUS Access-Request Denial of Service	Low	Gentoo Linux Security Advisory, GLSA 200409-29, September 22, 2004 **US-CERT Vulnerability Note VU#541574, October 11, 2004**
GNU gettext 0.14.1	A vulnerability exists due to the insecure creation of temporary files, which could possible let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Gentoo: http://security.gentoo.org/glsa/glsa-200410-10.xml** There is no exploit code required.	GNU GetText Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 **Gentoo Linux Security Advisory, GLSA 200410-10, October 10, 2004**
INCOGEN, Inc. BugPort 1.0 90-1.0 99, 1.101, 1.108, 1.109, 1.117, 1.119, 1.125, 1.129, 1.133	A vulnerability exists due improper handling of file attachments. This could possibly lead to the execution of arbiter code. Upgrades available at: http://freshmeat.net/redir/bugport/43537/url_tgz/bugport-current.tar.gz We are not aware of any exploits for this vulnerability.	BugPort File Attachment	High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011543, October 5, 2004
Jem Berkes renattach 1.2, 1.2.1	A vulnerability exists in the the '--pipe' command, which could potentially let a remote malicious user execute arbitrary commands. Updates available at: http://freshmeat.net/redir/renattach/8951/url_tgz/renattach-1.2.2.tar.gz There is no exploit code required.	Renattach '--pipe' Input Validation	High	Secunia Advisory, SA12778, October 11, 2004

Multiple Vendors
Apache Software Foundation Apache 2.0.50 & prior; Gentoo Linux 1.4;
RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3;
Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1
	A remote Denial of Service vulnerability exists in the Apache mod_dav module when an authorized malicious user submits a specific sequence of LOCK requests.
	Update available at: http://httpd.apache.org/
	Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml
	RedHat: ftp://updates.redhat.com/enterprise
	Trustix: ftp://ftp.trustix.org/pub/trustix/updates/
	Conectiva: ftp://atualizacoes.conectiva.com.br/
	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Debian: http://security.debian.org/pool/updates/main/liba/
	There is no exploit code required; however, Proof of Concept exploit has been published.
		Apache mod_dav Remote Denial of Service
		CVE Name: CAN-2004-0809
			Low	SecurityTracker Alert ID, 1011248, September 14, 2004
				Conectiva Linux Security Announcement, CLA-2004:868, September 23, 2004
				Fedora Update Notification, FEDORA-2004-313, September 23, 2004
				Debian Security Advisory DSA 558-1 , October 6, 2004

Multiple Vendors Gentoo Linux 1.4; KDE KDE 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3; MandrakeSoft Linux Mandrake 9.2 amd64, 9.2, 10.0 AMD64, 10.0	A vulnerability exists due to insufficient validation of ownership of temporary directories, which could let a malicious user cause a Denial of Service, overwrite arbitrary files, or obtain elevated privileges. KDE: ftp://ftp.kde.org/pub/kde/security_patches/post-3.0.5b-kdelibs-kstandarddirs.patch Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-13.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/	KDE Insecure Temporary Directory Symlink CVE Name: CAN-2004-0689	Low/Medium (Low if a DoS)	KDE Security Advisory,August 11, 2004 Fedora Update Notifications, FEDORA-2004-290 & 291, September 8, 2004 Conectiva Linux Security Announcement,

	Fedora:http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat: http://rhn.redhat.com/errata/RHSA-2004-412.html** There is no exploit code required.			CLA-2004:864, September 13, 2004 **RedHat Security Advisory, RHSA-2004:412-11, October 5, 2004**
Multiple Vendors Apple Mac OS X 10.2-10.2.8, 10.3 - 10.3.5, OS X Server 10.2-10.2.8, 10.3 - 10.3.5; Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4-5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.21	A vulnerability exists in 'error_log' when certain methods of remote printing are carried out by an authenticated malicious user, which could disclose user passwords. Update available at: http://www.cups.org/software.php Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04829&platform=osx&method=sa/SecUpd2004-09-30Jag.dmg http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04830&platform=osx&method=sa/SecUpd2004-09-30Pan.dmg Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-06.xml There is no exploit code required.	CUPS Error_Log Password Disclosure CVE Name: CAN-2004-0923	Medium	Apple Security Update, APPLE-SA-2004-09-30, October 4, 2004 Fedora Update Notification, FEDORA-2004-331, October 5, 2004 Gentoo Linux Security Advisory, GLSA 200410-06, October 9, 2004
Multiple Vendors Easy Software Products CUPS 1.1.14-1.1.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A Denial of Service vulnerability exists in 'scheduler/dirsvc.c' due to insufficient validation of UDP datagrams. Update available at: http://www.cups.org/software.php Debian: http://security.debian.org/pool/updates/main/c/cupsys/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ ALTLinux: http://altlinux.com/index.php?module=sisyphus&package=cups Gentoo: http://security.gentoo.org/glsa/glsa-200409-25.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Apple: http://www.apple.com/support/security/security_updates.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ **Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57646-1&searchclause=** A Proof of Concept exploit has been published.	CUPS Browsing Denial of Service CVE Name: CAN-2004-0558	Low	SecurityTracker Alert ID, 1011283, September 15, 2004 ALTLinux Advisory, September 17, 2004 Gentoo Linux Security Advisory GLSA 200409-25, September 20, 2004 Slackware Security Advisory, SSA:2004-266-01, September 23, 2004 Fedora Update Notification, FEDORA-2004-275, September 28, 2004 Apple Security Update, APPLE-SA-2004-09-30, October 4, 2004 **Sun(sm) Alert Notification, 57646, October 7, 2004**
Multiple Vendors Enlightenment Imlib2 1.0-1.0.5, 1.1, 1.1.1; ImageMagick ImageMagick 5.4.3, 5.4.4 .5, 5.4.8 .2-1.1.0 , 5.5.3 .2-1.2.0, 5.5.6 .0- 2003040, 5.5.7,6.0.2; Imlib Imlib 1.9-1.9.14	Multiple buffer overflow vulnerabilities exist in the Iimlib/Imlib2 libraries when handling malformed bitmap images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Imlib: http://cvs.sourceforge.net/viewcvs.py/enlightenment/e17/ ImageMagick: http://www.imagemagick.org/www/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200409-12.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-465.html SuSE:ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/ Conectiva: ftp://atualizacoes.conectiva.com.br/	IMLib/IMLib2 Multiple BMP Image Decoding Buffer Overflows CVE Names: CAN-2004-0817, CAN-2004-0802	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 1, 2004 Gentoo Linux Security Advisory, GLSA 200409-12, September 8, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:089, September 8, 2004 Fedora Update Notifications, FEDORA-2004-300 &301, September 9,

	Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57648-1&searchclause= http://sunsolve.sun.com/search/document.do?assetkey=1-26-57645-1&searchclause= **TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/** We are not aware of any exploits for this vulnerability.			2004 Turbolinux Security Advisory, TLSA-2004-27, September 15, 2004 RedHat Security Advisory, RHSA-2004:465-08, September 15, 2004 Debian Security Advisories, DSA 547-1 & 548-1, September 16, 2004 Conectiva Linux Security Announcement, CLA-2004:870, September 28, 2004 Sun(sm) Alert Notifications, 57645 & 57648, September 20, 2004 **Turbolinux Security Announcement, October 5, 2004**
Multiple Vendors Gentoo Linux 1.4; RedHat Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1, Desktop 3.0, t Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, 2.1 IA64, 2.1, AS 3, AS 2.1 IA64, AS 2.1' Trolltech Qt 3.0, 3.0.5, 3.1, 3.1.1, 3.1.2, 3.2.1, 3.2.3, 3.3 .0, 3.3.1, 3.3.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'read_dib()' function when handling 8-bit RLE encoded BMP files, which could let a malicious user execute arbitrary code; and buffer overflow vulnerabilities exist in the in the XPM, GIF, and JPEG image file handlers, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/q/qt-copy/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-20.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/kde/qt-3.1.2-i486-4.tgz SuSE: ftp://ftp.suse.com/pub/suse/i386/update Trolltech Upgrade: http://www.trolltech.com/download/index.html TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57637-1&searchclause=security Conectiva: ftp://atualizacoes.conectiva.com.br/ **RedHat: http://rhn.redhat.com/errata/RHSA-2004-478.html http://rhn.redhat.com/errata/RHSA-2004-479.html** **SuSE: ftp://ftp.suse.com/pub/suse/** Proof of Concept exploit has been published.	QT Image File Buffer Overflows CVE Names: CAN-2004-0691, CAN-2004-0692, CAN-2004-0693	High	Secunia Advisory, SA12325, August 10, 2004 Sun Alert ID: 57637, September 3, 2004 Conectiva Linux Security Announcement, CLA-2004:866, September 22, 2004 **RedHat Security Advisories, RHSA-2004:478-13 & RHSA-2004:479-05, October 4 & 6, 2004** **SUSE Security Announcement, SUSE-SA:2004:035, October 5, 2004**
Multiple Vendors KDE 3.2.3 and prior	A frame injection vulnerability exists in the Konqueror web browser that allows websites to load web pages into a frame of any other frame-based web page that the user may have open. A malicious website could abuse Konqueror to insert its own frames into the page of an otherwise trusted website. As a result, the user may unknowingly send confidential information intended for the trusted website to the malicious website. Source code patches have been made available which fix these vulnerabilities. Refer to advisory: http://www.kde.org/info/security/advisory-20040811-3.txt Gentoo: http://security.gentoo.org/glsa/glsa-200408-13.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora:http://download.fedora.redhat.com/pub/fedora/linux/core/updates/	Konqueror Frame Injection Vulnerability CVE Name: CAN-2004-0721	Low	KDE Security Advisory 20040811-3, August 11, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:086, August 21, 2004 Fedora Update Notifications, FEDORA-2004-290 & 291,

	RedHat: http://rhn.redhat.com/errata/RHSA-2004-412.html A Proof of Concept exploit has been published.			September 8, 2004 Conectiva Linux Security Announcement, CLA-2004:864, September 13, 2004 **RedHat Security Advisory, RHSA-2004:412-11, October 5, 2004**
Multiple Vendors LinuxPrinting.org Foomatic-Filters 3.03.0.2, 3.1; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A vulnerability exists in the foomatic-rip print filter due to insufficient validation of command-lines and environment variables, which could let a remote malicious user execute arbitrary commands. Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-24.xml **Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57646-1&searchclause=** We are not aware of any exploits for this vulnerability.	LinuxPrinting.org Foomatic-Filter Arbitrary Code Execution CVE Name: CAN-2004-0801	High	Secunia Advisory, SA12557, September 16, 2004 Fedora Update Notification, FEDORA-2004-303, September 21, 2004 Gentoo Linux Security Advisory, GLSA 200409-24, September 17, 2004 **Sun(sm) Alert Notification, 57646, October 7, 2004**
Multiple Vendors Samba Samba 2.2 a, 2.2 .0a, 2.2 .0, 2.2.1 a, 2.2.2, 2.2.3 a, 2.2.3-2.2.9, 2.2.11, 3.0, alpha, 3.0.1-3.0.5; MandrakeSoft Corporate Server 2.1, x86_64, 9.2, amd64	A vulnerability exists due to input validation errors in 'unix_convert()' and 'check_name()' when converting DOS path names to path names in the internal filesystem, which could let a remote malicious user obtain sensitive information. Samba: http://download.samba.org/samba/ftp/patches/security/ http://us1.samba.org/samba/ftp/old-versions/samba-2.2.12.tar.gz Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Debian: http://security.debian.org/pool/updates/main/s/samba/** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **RedHat: http://rhn.redhat.com/errata/RHSA-2004-498.html** **SuSE: ftp://ftp.suse.com/pub/suse/** **Trustix: ftp://http.trustix.org/pub/trustix/updates/** There is no exploit code required.	Samba Remote Arbitrary File Access CVE Name: CAN-2004-0815	Medium	iDEFENSE Security Advisory, September 30, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:104, October 1, 2004** **Debian Security Advisory DSA 600-1, October 7, 2004** **RedHat Security Advisory, RHSA-2004:498-04, October 1, 2004** **SUSE Security Announcement, SUSE-SA:2004:035, October 5, 2004** **Trustix Secure Linux Security Advisory, TSLSA-2004-0051, October 1, 2004**
Nathaniel Bray Yeemp 0.5, 0.5.1, 0.9.9	A vulnerability exists due to insufficient verification of public keys when a file is transferred, which could let a remote malicious user spoof sender information and potentially execute arbitrary code. Upgrades available at: http://deekoo.net/technocracy/yeemp/http://deekoo.net/technocracy/yeemp/ There is no exploit code required.	Nathaniel Bray Yeemp File Transfer Public Key Verification Bypass	Medium/ High (High if arbitrary code can be executed)	SecurityFocus, October 7, 2004
Squid-cache.org Squid 2.5-STABLE6, 3.0-PRE3-20040702; when compiled with SNMP support	A remote Denial of Service vulnerability exists in the 'asn_parse_header()' function in 'snmplib/asn1.c' due to an input validation error when handling certain negative length fields. Updates available at: http://www.squid-cache.org/ We are not aware of any exploits for this vulnerability.	Squid Remote Denial of Service CVE Name: CAN-2004-0918	Low	iDEFENSE Security Advisory, October 11, 2004

Ulrich Callmeier Net-Acct 0.x	A vulnerability exists in the 'write_list()' and 'dump_curr_list()' functions due to the insecure creation of temporary files, which could let a malicious user modify information. Patch available at: http://exorsus.net/projects/net-acct/net-acct-notempfiles.patch **Debian: http://security.debian.org/pool/updates/main/n/net-acct/** We are not aware of any exploits for this vulnerability.	Net-acct Insecure Temporary File CVE Name: CAN-2004-0851	Medium	Secunia Advisory, September 7, 2004 Debian Security Advisory DSA 559-1, October 6, 2004
XFree86 Project OpenBSD; xdm CVS	A vulnerability exists in xdm because even though 'DisplayManager.requestPort' is set to 0 xdm will open a 'chooserFd' TCP socket on all interfaces, which could lead to a false sense of security. Patch available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/008_xdm.patch Gentoo: http://security.gentoo.org/glsa/glsa-200407-05.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **RedHat: http://rhn.redhat.com/errata/RHSA-2004-478.html** Currently we are not aware of any exploits for this vulnerability.	XFree86 XDM RequestPort False Sense of Security CVVE Name: CAN-2004-0419	Medium	Secunia Advisory, SA11723, May 30, 2004 **RedHat Security Advisory, RHSA-2004:478-13, October 4, 2004**
xinehq.de xine 0.5.2 - 0.5.x; 0.9.x; 1-alpha.x; 1-beta.x; 1-rc - 1-rc5	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the DVD subpicture component, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the VideoCD functionality when reading ISO disk labels, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists when handling text subtitles, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/xine/xine-lib-1-rc6a.tar.gz?download Gentoo: http://security.gentoo.org/glsa/glsa-200409-30.xml **Mandrake: http://www.mandrakesecure.net/en/ftp.php** We are not aware of any exploits for this vulnerability.	Xine-lib Multiple Buffer Overflows	High	Secunia Advisory, SA12602 September 20, 2004 Gentoo Linux Security Advisory, GLSA 200409-30, September 22, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:105, October 6, 2004**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
brooky.com CubeCart 2.0.1	A vulnerability exists due to insufficient sanitization of the 'cat_id' parameter, 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; however, a Proof of Concept exploit has been published.	CubeCart Input Validation	Medium	Secunia Advisory, SA12764, October 8, 2004
cjoverkill.icefire.org CJOverkill 4.0.3	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of input passed to the 'tms' array parameter and 'url' parameter in 'trade.php,' which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	CJOverkill Cross-Site Scripting	High	SECUNIA ADVISORY ID, SA12786, October 11, 2004
Content Management System DCP-Portal 3.7, 4.0, 4.1, 4.2, 4.5.1, 5.0.1, 5.0.2, 5.1, 5.2, 5.3, 5.3.1, 5.3.2	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of input passed to various parameters in the 'calendar.php,' 'index.php,' 'announcement.php,' 'news.php,' and 'contents.php' scripts, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability exists due to insufficient sanitization of input passed to various variables in several PHP scripts via HTTP POST requests, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability exists in 'PHPSESSID' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	DCP-Portal Multiple Cross-Site Scripting Vulnerabilities	High	Maxpatrol Security Advisory, October 6, 2004
Duware DUclassified	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the 'login' form due to insufficient validation of the 'password' variable, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the admin page due to insufficient validation of the 'user' variable, which could let a remote malicious user obtain administrative access; and a vulnerability exists in the 'cat_id' parameter in 'adDetail.asp,' which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing.	DUclassified Input Validation Vulnerabilities	High	SecurityTracker Alert ID, 1011596, October 11, 2004

	Proofs of Concept exploits have been published.			
Duware DUclassmate	A vulnerability exists in the 'account.asp' script due to insufficient authentication of user-supplied password change requests, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	DUclassmate Password Change Request	Medium	SecurityTracker Alert ID, 1011597, October 11, 2004
DUware DUforum	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the 'login' form due to insufficient validation of the 'password' variable, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in 'messages.asp' due to insufficient validation of the 'FOR_ID' parameter and in 'messageDetail.asp' due to insufficient validation of the 'MSG_ID' parameter, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	DUforum Input Validation Vulnerabilities	High	SecurityTracker Alert ID, 1011595, October 11, 2004
IBM DB2 Universal Database for AIX 8.0, 8.1, DB2 Universal Database for HP-UX 8.0, 8.1, DB2 Universal Database for Linux 8.0, 8.1, DB2 Universal Database for Solaris 8.0, 8.1, DB2 Universal Database for Windows 8.0, 8.1	Twenty vulnerabilities exist most of which are buffer overflows that could let a remote malicious user execute arbitrary code. (Details were not specified at this time). Patches available at: http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html We are not aware of any exploits for this vulnerability.	IBM DB2 Multiple Buffer Overflows	High	NGSSoftware Insight Security Research Advisory, October 5, 2004
Icecast.org Icecast 2.0, 2.0.1	A buffer overflow vulnerability exists due to a boundary error in the parsing of HTTP headers, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://svn.xiph.org/releases/icecast/icecast-2.0.2.tar.gz **Exploit scripts have been published.**	Icecast Server HTTP Header Buffer Overflow	High	SecurityTracker Alert ID. 1011439, September 29, 2004 **Packet Storm, October 7, 2004**
Invision Power Services Invision Board 2.0	A Cross-Site Scripting vulnerability exists in 'index.php' due to insufficient sanitization of input passed via the 'Referer' header, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Invision Power Board Referer Cross-Site Scripting	High	Secunia Advisory, SA12740, October 6, 2004
Macromedia Coldfusion 6.0, 6.1; MX	A vulnerability exists in the default configuration because the 'CFOBJECT' tag and the 'CreateObject' function are accessible to all developers, which could let a malicious user obtain elevated privileges. Workaround information available at: http://livedocs.macromedia.com/coldfusion/6.1/htmldocs/appsecur.htm We are not aware of any exploits for this vulnerability.	Macromedia ColdFusion Default Configuration Elevated Privileges	Medium	Macromedia Security Advisory, MPSB04-10, October 11, 2004
Macromedia ColdFusion MX 6.1	A vulnerability exists due to an access validation issue, which could let a remote malicious user obtain sensitive information. Patch available at: http://www.macromedia.com/devnet/security/security_zone/mpsb04-09.html There is no exploit code required.	Macromedia ColdFusion MX Remote File Content Disclosure CVE Name: CAN-2004-0928	Medium	Securiteam, October 6, 2004
Matthew Phillips Sticker 3.1 .0 beta 1	A vulnerability exists due to a flaw in the application, which could let an unauthenticated remote malicious user send messages to groups. Upgrade available at: http://www.tickertape.org/download/get.jsp?package=sticker-src-3.1.0b2.zip There is no exploit code required.	Sticker Unauthorized Secure Message	Medium	SecurityTracker Alert ID, 1011580, October 9, 2004

Mozilla.org
Mozilla 1.6;
Mozilla 1.7.x;
Mozilla Firefox 0.x
	A Denial of Service vulnerability exists in which arbitrary root certificates are imported silently without presenting users with a import dialog box. Due to another problem, this can e.g. be exploited by malicious websites or HTML-based emails to prevent users from accessing valid SSL sites.
	Workaround: Check the certificate store and delete untrusted certificates if an error message is displayed with error code -8182 ("certificate presented by [domain] is invalid or corrupt") when attempting to access a SSL-based website.
	SuSE: ftp://ftp.suse.com/pub/suse/
	Currently, we are not aware of any exploits for this vulnerability.
		Mozilla / Firefox Certificate Store Corruption Vulnerability
		CVE Name: CAN-2004-0758
			Low	Secunia Advisory, SA12076, July 16, 2004
				Bugzilla Bug 24900, July 14, 2004
				SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004

Mozilla.org	A spoofing vulnerability exists that could allow malicious sites to abuse SSL certificates	Mozilla / Mozilla	Medium	Cipher.org, July

Mozilla Firefox 0.9.2 and Mozilla 1.7.1 on Windows Mozilla Firefox 0.9.2 on Linux	of other sites. An attacker could make the browser load a valid certificate from a trusted website by using a specially crafted "onunload" event. The problem is that Mozilla loads the certificate from a trusted website and shows the "secure padlock" while actually displaying the content of the malicious website. The URL shown in the address bar correctly reads that of the malicious website. An additional cause has been noted due to Mozilla not restricting websites from including arbitrary, remote XUL (XML User Interface Language) files. Workaround: Do not follow links from untrusted websites and verify the correct URL in the address bar with the one in the SSL certificate. **SuSE: ftp://ftp.suse.com/pub/suse/** A Proof of Concept exploit has been published.	Firefox "onunload" SSL Certificate Spoofing CVE Name: CAN-2004-076		25, 2004 Secunia, SA12160, July 26, 2004; SA12180, July 30, 2004 **SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004**
Mozilla.org Mozilla 1.6 & prior; Netscape 7.0, 7.1, and prior	A input validation vulnerability exists in the SOAPParameter object constructor in Netscape and Mozilla which allows execution of arbitrary code. The SOAPParameter object's constructor contains an integer overflow that allows controllable heap corruption. A web page can be constructed to leverage this into remote execution of arbitrary code. Upgrade to Mozilla 1.7.1 available at: http://www.mozilla.org/products/mozilla1.x/ **SuSE: ftp://ftp.suse.com/pub/suse/** We are not aware of any exploits for this vulnerability.	Netscape/Mozilla SOAPParameter Constructor Integer Overflow Vulnerability CVE Name: CAN-2004-0722	High	iDEFENSE Security Advisory, August 2, 2004 Bugzilla Bug 236618 **SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004**
Mozilla.org Firefox Preview Release, 0.8, 0.9 rc, 0.9-0.9.3, 0.10	A vulnerability exists due to an error when downloading files, which could let a remote malicious user delete all content in the download directory. Upgrade available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/0.10.1/firefox-1.0PR-source.tar.bz2 Patch available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/0.10.1/patches/259708.xpi There is no exploit code required.	Mozilla Firefox DATA URI File Deletion	Medium	SecurityFocus, October 2, 2004
Mozilla.org Mandrakesoft Slackware Mozilla 1.7 and prior; Firefox 0.9 and prior; Thunderbird 0.7 and prior	Multiple vulnerabilities exist in Mozilla, Firefox, and Thunderbird that could allow a malicious user to conduct spoofing attacks, compromise a vulnerable system, or cause a Denial of Service. These vulnerabilities include buffer overflow, input verification, insecure certificate name matching, and out-of-bounds reads. Upgrade to the latest version of Mozilla, Firefox, or Thunderbird available at: http://www.mozilla.org/download.html Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.667659 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:082 RedHat: http://rhn.redhat.com/errata/RHSA-2004-421.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-26.xml HP: http://h30097.www3.hp.com/internet/download.htm **SuSE: ftp://ftp.suse.com/pub/suse/** We are not aware of any exploits for this vulnerability.	Mozilla/Firefox/ Thunderbird Multiple Vulnerabilities CVE Name: CAN-2004-0757, CAN-2004-0759, CAN-2004-0761 CAN-2004-0765	High	Secunia, SA10856, August 4, 2004 US-CERT Vulnerability Note VU#561022 RedHat Security Advisory, RHSA-2004:421-17, August 4, 2004 SGI Security Advisory, 20040802-01-U, August 14, 2004 Gentoo Linux Security Advisory, GLSA 200409-26, September 20, 2004 HP Security Bulletin, HPSBTU01081, October 5, 2004 **SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004**
Mozilla.org Mozilla 0.x, 1.0-1.7.x, Firefox 0.x, Thunderbird 0.x; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2	Multiple vulnerabilities exist: buffer overflow vulnerabilities exist in 'nsMsgCompUtils.cpp' when a specially crafted e-mail is forwarded, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to insufficient restrictions on script generated events, which could let a remote malicious user obtain sensitive information; a buffer overflow vulnerability exists in the 'nsVCardObj.cpp' file due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'nsPop3Protocol.cpp' due to boundary errors, which could let a remote malicious user execute arbitrary code; a heap overflow vulnerability exists when handling non-ASCII characters in URLs, which could let a remote malicious user execute arbitrary code; multiple integer overflow vulnerabilities exist in the image parsing routines due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a cross-domain scripting vulnerability exists because URI links dragged from one browser window and	Mozilla Multiple Remote Vulnerabilities CVE Names: CAN-2004-0902, CAN-2004-0903, CAN-2004-0904, CAN-2004-0905, CAN-2004-0908	Medium/ High (High if arbitrary code can be executed)	Technical Cyber Security Alert TA04-261A, September 17, 2004 US-CERT Vulnerability Notes VU#414240, VU#847200, VU#808216, VU#125776,

	dropped into another browser window will bypass same-origin policy security checks, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because unsafe scripting operations are permitted, which could let a remote malicious user manipulate information displayed in the security dialog. Updates available at: http://www.mozilla.org/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-26.xml HP: http://h30097.www3.hp.com/internet/download.htm RedHat: http://rhn.redhat.com/errata/RHSA-2004-486.html **SuSE: ftp://ftp.suse.com/pub/suse/** Proofs of Concept exploits have been published.			VU#327560, VU#651928, VU#460528, VU#113192, September 17, 2004 Gentoo Linux Security Advisory, GLSA 200409-26, September 20, 2004 RedHat Security Bulletin, RHSA-2004:486-18, September 30, 2004 HP Security Bulletin, HPSBTU01081, October 5, 2004 **SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004**
Multiple Vendors AJ-Fork AJ-Fork 16-; CutePHP CuteNews 0.88, 1.3-1.3.2, 1.3.6	A vulnerability exists due to insecure default file permissions, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. **Exploit script has been published.**	AJ-Fork Insecure Default Permissions	Medium	Bugtraq, October 1, 2004. **Packet Storm, October 7, 2004**
Multiple Vendors Gentoo Linux 0.5, 0.7, 1.1 a, 1.2, 1.4, _rc1-rc3; PHP PHP 4.0-4.0.7, 4.1.0-4.1.2, 4.2.0-4.2.3, 4.3-4.3.8, 5.0.0, 5.0.1	A vulnerability exists in the array parsing functions of the 'php_variables.c' PHP source file, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://www.php.net/downloads.php#v5 Gentoo: http://security.gentoo.org/glsa/glsa-200410-04.xml A Proof of Concept exploit has been published.	PHP PHP_Variables Remote Memory Disclosure	Medium	SecurityFocus, October 6, 2004
Multiple Vendors IBM Trading Partner Interchange (TPI) 4.2.1, 4.2.2; Jetty Jetty 3.1.6, 3.1.7, 4.1 .0RC4, 4.1 .0, 4.1.1, 4.2.4-4.2.7, 4.2.9, 4.2.11, 4.2.12, 4.2.14-4.2.19	A Directory Traversal vulnerability exists due to insufficient sanitization of HTTP URIs requests, which could let a remote malicious user obtain sensitive information. IBM: http://www-1.ibm.com/support/docview.wss?uid=swg21178665 There is no exploit code required.	Jetty Directory Traversal	Medium	SecurityFocus, October 5, 2004
MySQL AB MaxDB 7.5.00.16, 7.5.00.15, 7.5.00.14, 7.5.00.12, 7.5.00.11, 7.5.00.08, SAP DB 7.5	A remote Denial of Service vulnerability exists due to an input validation error in the 'IsAscii7()' function. Upgrade available at: http://dev.mysql.com/downloads/maxdb/7.5.00.html There is no exploit code required.	MySQL MaxDB WebDBM Server Name Denial of Service CVE Name: CAN-2004-0931	Low	Secunia Advisory, SA12756, October 7, 2004
MySQL.com MySQL 3.x, 4.x	Two vulnerabilities exist: a vulnerability exists due to an error in 'ALTER TABLE ... RENAME' operations because the 'CREATE/INSERT' rights of old tables are checked, which potentially could let a remote malicious user bypass security restrictions; and a remote Denial of Service vulnerability exists when multiple threads issue 'alter' commands against 'merge' tables to modify the 'union.' Updates available at: http://dev.mysql.com/downloads/mysql/ Debian: http://security.debian.org/pool/updates/main/m/mysql We are not aware of any exploits for this vulnerability.	MySQL Security Restriction Bypass & Remote Denial of Service CVE Names: CAN-2004-0835, CAN-2004-0837	Low/ Medium (Low if a DoS; and Medium if security restrictions can be bypassed)	Secunia Advisory, SA12783, October 11, 2004
PNG Development Group Conectiva Debian Fedora Gentoo Mandrakesoft RedHat SuSE Sun Solaris HP-UX GraphicsMagick ImageMagick	Multiple vulnerabilities exist in the libpng library which could allow a remote malicious user to crash or execute arbitrary code on an affected system. These vulnerabilities include: • libpng fails to properly check length of transparency chunk (tRNS) data, • libpng png_handle_iCCP() NULL pointer dereference, • libpng integer overflow in image height processing, • libpng png_handle_sPLT() integer overflow, • libpng png_handle_sBIT() performs insufficient bounds checking, • libpng contains integer overflows in progressive display image reading. If using original, update to libpng version 1.2.6rc1 (release candidate 1) available at: http://www.libpng.org/pub/png/libpng.html	Multiple Vulnerabilities in libpng CVE Names: CAN-2004-0597 CAN-2004-0598 CAN-2004-0599	High	US-CERT Technical Cyber Security Alert TA04-217A, August 4, 2004 US-CERT Vulnerability Notes VU#160448, VU#388984,

Slackware libpng 1.2.5 and 1.0.15	Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000856 Debian: http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00139.html Gentoo: http://security.gentoo.org/glsa/glsa-200408-03.xml Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:079 RedHat http://rhn.redhat.com/ SuSE: http://www.suse.de/de/security/2004_23_libpng.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Sun Solaris: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57617 HP-UX: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01065 GraphicsMagick: http://www.graphicsmagick.org/www/download.html ImageMagick: http://www.imagemagick.org/www/download.html Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.439243 Yahoo: http://messenger.yahoo.com/ **SuSE: ftp://ftp.suse.com/pub/suse** A Proof of Concept exploit has been published.			VU#817368, VU#236656, VU#477512, VU#286464, August 4, 2004 **SUSE Security Announcement, SUSE-SA:2004:035, October 5, 2004**
RealNetworks Helix Universal Gateway 9.0, 9.0.2 .881, Helix Universal Mobile Gateway 10.1.1 .120, 10.3.1 .716, Helix Universal Mobile Server 10.1.1 .120, 10.3.1 .716	A remote Denial of Service vulnerability exists due to insufficient validation of HTTP requests. Upgrades available at: http://www.service.real.com/help/faq/security/security100704.html There is no exploit code required.	Real Networks Helix Universal Server Remote Denial of Service CVE Name: CAN-2004-0774	Low	SecurityFocus, October 7, 2004
The BNC Project BNC 2.2.4, 2.4.6, 2.4.8, 2.6, 2.6.2, 2.8.8	A buffer overflow vulnerability exists due to a flaw when processing the backspace character, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://www.gotbnc.com/files/bnc2.8.9.tar.gz We are not aware of any exploits for this vulnerability.	BNC Buffer Overflow	High	SecurityTracker Alert ID, 1011583, October 9, 2004
TurboTrafficTrader.com Nitro 1.0	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists in 'ttt-webmaster.php' due to insufficient sanitization of the 'msg' array parameter and 'siteurl' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in 'security.inc.php' due to insufficient sanitization of the 'ttt_admin' cookie parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Turbo Traffic Trader Nitro Cross-Site Scripting & SQL Injection	High	SecurityTracker Alert ID, 1011609, October 11, 2004
WordPress WordPress 1.2	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient verification of user-supplied input passed to certain parameters in various scripts, which could let a remote malicious user execute arbitrary HTML and script code. **Upgrade available at: http://wordpress.org/latest.tar.gz** There is no exploit code required; however, Proofs of Concept exploits have been published.	Wordpress Multiple Cross-Site Scripting	High	Bugtraq, September 27, 2004 **Secunia Advisory, SA12773, October 11, 2004**
Yves Goergen BlackBoard Internet Newsboard System 1.5.1	Several vulnerabilities exist: a vulnerability exists in the the '/bb_lib/admin.inc.php' file due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because the full path to certain scripts is exposed, which could let a remote malicious user obtain sensitive information. Patch available at: http://blackboard.unclassified.de/release/update/patch-1.5.1-h.zip A Proof of Concept exploit has been published.	BlackBoard Internet Newsboard System Remote File Include	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID: 1011551, October 6, 2004
Zanfi Solutions ZanfiCmsLite 1.1	Several vulnerabilities exist: a vulnerability exists in 'index.php' due to insufficient verification of the 'inc' parameter, which could let a remote malicious user execute arbitrary PHP code; and a vulnerability exists because a remote malicious user can request any of several scripts directly which could disclose sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Zanfi CMS Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011612, October 11, 2004

Recent Exploit Scripts/Techniques

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

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

Date of Exploit (Reverse Chronological Order)	Exploit Name	Workaround or Patch Available	Script Description
October 13, 2004	101_ypops.cpp	No	Exploit for the remote buffer overflows in both the POP3 and SMTP services of the YahooPOPs application.
October 13, 2004	AntiExploit-1.3b5.tar.gz	N/A	An exploit scanner that detect local intruders. It scans for over 3900 suspicious files, has daily database updates, and will act if a file is accessed. It uses the dazuko kernel module, which is also used by clamAV, Amavis, and other virus scanners.
October 13, 2004	flashmsg.zip	No	Proof of Concept exploit for the Jera Technology Flash Messaging Server Remote Denial of Service vulnerability.
October 13, 2004	gosmart.txt	No	Exploit examples for the GoSmart Message Board Cross-Site Scripting vulnerabilities.
October 13, 2004	intro_to_shellcoding.pdf	N/A	Introduction to Shellcode: How to exploit buffer overflows. A very thorough and well written paper on how it all works that includes step by step examples from vulnerability discovery to a finished exploit. The paper focuses on x86 Intel syntax assembly under Linux.
October 13, 2004	jc-wepcrack.tar.gz	N/A	jc-wepcrack is a distributed WEP cracker that uses its own sockets-based protocol for communication.
October 13, 2004	lithsec.zip	No	Remote Proof of Concept exploit for the Monolith Games Buffer Overflow vulnerability.
October 13, 2004	PolymorphicEvasion.txt	N/A	White paper discussing ways to evade detection of polymorphic shellcode.
October 13, 2004	prismstumbler-0.7.3.tar.bz2	N/A	Prismstumbler is software that finds 802.11 (W-LAN) networks. It comes with an easy to use GTK2 frontend and is small enough to fit on a small portable system. It is designed to be a flexible tool to find as much information about wireless LAN installations as possible.
October 13, 2004	remoteActivate.txt	N/A	Information on how to manipulate registry keys once a command shell is obtained to invoke the Remote Desktop functionality of XP.
October 13, 2004	shadowmac-1.0.tar.gz	N/A	A kernel patch for spoofing MAC addresses under Mac OS X.
October 13, 2004	tridcomm13.txt	No	Exploit for the TriDComm FTP Server Directory Traversal vulnerability.
October 13, 2004	turboTraffic.txt	No	Exploit for the Turbo Traffic Trader Nitro Cross-Site Scripting & SQL Injection vulnerability.
October 13, 2004	vymesbof.zip	Yes	Proof of Concept exploit for the VyPRESS Messenger Remote Buffer Overflow vulnerability.
October 8, 2004	lithsecGameEnginePoC.zip	No	Proof of Concept exploit for the Monolith Lithtech Game Engine Remote Buffer Overflow vulnerability.
October 8, 2004	SSL_PCT_EXPLOITATION_ANALYSIS.PDF	N/A	Whitepaper analysis of the THCIISLAME SSL/PCT bug, how the bug was exploited and how to use it. Included is a small introduction to generic exploit coding.
October 7, 2004	adv07-y3dips-2004.txt	No	Exploit for the AJ-Fork Insecure Default Permissions vulnerability.
October 7, 2004	aircrack-2.1.tgz	N/A	An 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have been gathered.
October 7, 2004	flashmsg.tar	No	Exploit for the Jera Technology Flash Messaging Server Remote Denial of Service vulnerability.
October 7, 2004	iceexec.rar priv8icecast.pl iceexec2.zip	Yes	Scripts that exploit the Icecast Server HTTP Header Buffer Overflow vulnerability.
October 7, 2004	pads-1.1.3.tar.gz	N/A	Pads is a signature based detection engine used to passively detect network assets.
October 7, 2004	REALSERVER_EXPLOIT_ANALYSIS.PDF	N/A	Whitepaper analysis on how to use the THCREALBAD Realserver exploit and how it works. Additionally, a real life intrusion with this exploit is shown with what to do after root privileges are achieved.
October 7, 2004	sacred_jpg.c	Yes	Script that exploits the Microsoft JPEG Processing Buffer Overflow vulnerability.
October 2, 2004	ipSwitchWhatsUpGoldBufferOverflowExpl.pl NotmuchG.pl	Yes	Script that exploits the WhatsUp Gold Remote Buffer Overflow vulnerability.
October 7, 2004	tcptrack-1.1.3.tar.gz	N/A	A packet sniffer that passively watches for connections on a specified network interface, tracking their states and listing them in a manner similar to the top command. It displays source and destination addresses and ports, connection state, idle time, and bandwidth usage.

[back to top]

Trends

- The SANS Institute has released their annual Twenty Most Critical Internet Security Vulnerabilities. The top 20 list is a consensus list of vulnerabilities that require immediate remediation. This list is located at http://www.sans.org/top20/. The list is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited vulnerable services in UNIX and Linux.
- To show how long viruses and worms live and spread on the Internet, Kaspersky Labs noted that its monthly Top 20 report for September was the first list this year that didn't contain malicious code from 2003. For more information, see http://www.kaspersky.com/news?id=153142439.
- Exploit codes for the Microsoft JPEG graphics handling vulnerability are still being released. If you have not patched for the MS04-28 vulnerability, please do so. See http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx for more information.

[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	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	Netsky-Z	Win32 Worm	Stable	April 2004
4	Netsky-D	Win32 Worm	Stable	March 2004
5	Bagle-AA	Win32 Worm	Increase	April 2004
6	Netsky-B	Win32 Worm	Slight Decrease	February 2004
7	Netsky-Q	Win32 Worm	Increase	March 2004
8	MyDoom-O	Win32 Worm	Increase	July 2004
9	Bagle-Z	Win32 Worm	New to Table	April 2004
10	MyDoom.M	Win32 Worm	Decrease	July 2004

Table Updated October 8, 2004

Viruses or Trojans Considered to be a High Level of Threat

- QHosts-18 / Downloader.Lunii: A new Trojan horse program that attacks and removes troublesome advertising software, known as "adware," is circulating on the Internet. When run, it attempts to kill off computer processes and delete files used by common adware programs. However, like other Trojan horse programs, it also modifies the configuration of Microsoft Windows machines and attempts to download files from a remote location. (PCWorld, October 7, 2004)
- Funner: Upon infection, this worm attempts to spread itself through the host's MSN Messenger contact list. In addition, the worm alters the Windows's host file, adding more than 900 URLs. Most security services categorize this attack as a nuisance and the spread in the wild is light. (eWeek, October 11, 2004)

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Berbew.K		Win32 Worm
Downloader-PZ		Trojan
Downloader-QG		Trojan
Downloader-QG.dr		Trojan: Dropper
Downloader-QI		Trojan
Downloader-QR		Trojan
Downloader-QU		Trojan
EXPL_JPGDOWN.B		Trojan: JPEG
EXPL_JPGDOWN.C	Trojan.Ducky.B	Trojan: JPEG
Lmir		Trojan
Nemsi.A	W32/Nemsi.A	Win32 Worm
Netsnake.H		Win32 Worm
QHosts-18	Downloader.Lunii Trojan.Win32.Qhost.n	Trojan
QHosts-18!hosts		Trojan
Trojan.AdRmove	Del-457 Trojan.AdRmove Trojan.Killfiles Trojan.Win32.KillFiles.fz	Trojan
Trojan.Comxt		Trojan
Trojan.Tannick		Trojan
Trojan.Webus.B		Trojan
W32.Bagz.B@mm	I-Worm.Bagz.a W32/Bagz.a@MM WORM_BAGZ.A W32/Bagz.b@MM	Win32 Worm
W32.Fili.A	WORM_FILI.A	Win32 Worm
W32.HLLW.Datrix	Bloodhound.Packed Bloodhound.W32.5 I-Worm.VB.q W32.Fili@mm	Visual Basic Worm
W32.Korgo.AE		Win32 Worm
W32.Mydoom.AD@mm		Win32 Worm
W32/Agobot-ZV		Win32 Worm

W32/Bagle-AC	I-Worm.Bagle.ac	Win32 Worm
W32/Darby-G		Win32 Worm
W32/Forbot-AY	Backdoor.Win32.Wootbot.gen W32/Gaobot.worm.gen.g WORM_WOOTBOT.GEN	Win32 Worm
W32/Forbot-AZ	WORM_WOOTBOT.GEN	Win32 Worm
W32/Forbot-BA		Win32 Worm
W32/Forbot-BD		Win32 Worm
W32/GregCenter		Win32 Worm
W32/Pikis-B	I-Worm.Pikis.c W32/Pikis!p2p	Win32 Worm
W32/Rbot-LT	Backdoor.Win32.Rbot.cd	Win32 Worm
W32/Rbot-LY		Win32 Worm
W32/Rbot-MI		Win32 Worm
W32/Sdbot.worm.bat.b		Win32 Worm
W32/Sdbot.worm.bat.b		Win32 Worm
W32/Sdbot-PZ	WORM_SDBOT.XN Backdoor.Win32.SdBot.05.bd	Win32 Worm
W32/Sdbot-QE	Win32.SdBot.gen W32/Sdbot.worm.gen.i WORM_SDBOT.WP	Win32 Worm
W97M.Kamal		MS Word Macro Virus
W97M.Prece.A		MS Word Macro Virus
Win32.Dluca.L	TrojanDownloader.Win32.Dluca.ai Win32/Dluca.L.Trojan	Win32 Worm
Win32.Secdrop.C	Downloader-NI TrojanDownloader.Win32.Small.qd Win32.Secdrop.C Win32/Istzone.H.Trojan	Win32 Worm
Win32.Secdrop.F	QLowZones-2.gen TrojanDropper.Win32.Agent.i Win32/Secdrop.F.Trojan	Win32 Worm
WORM_FUNNER.A	Funner MSN-Worm.Funner W32.Funner Win32.Funner.A W32/Funner.worm Win32/Funner.A.Worm	Win32 Worm
WORM_NOOMY.A		Win32 Worm

[back to top]

Last updated