Confidential

Subject: ISOC Blue Advisory – December 6, 2006 Excerpted from SANS Critical Vulnerabilities

Severity: Low

What: December 6, 2006 Excerpted from SANS Critical Vulnerabilities

Action: This is a notification from the ISOC for your information

Current Status: These are current as of 12/6/2006

ISOC Next Steps: If you have any questions please contact the ISOC.

Additional Information: December 6, 2006 Excerpted from SANS Critical Vulnerabilities

```
(1) HIGH: Apple Mac OS X Multiple Vulnerabilities (including Security Update
2006-007)
Affected:
Apple Mac OS X versions 10.4.8 and prior
Apple Mac OS X Server versions 10.4.8 and prior

Description: Apple Mac OS X contains multiple vulnerabilities that can
be exploited to compromise a vulnerable system. (1) The AirPort wireless
networking subsystem fails to properly handle malformed 802.11 frames.
By sending specially-crafted frames, an attacker could exploit this
vulnerability and execute arbitrary code with kernel privileges. This
issue is similar to one discussed in a previous @RISK newsletter entry.
(2) Apple Type Services (ATS), used for font and text processing,
contains a buffer overflow. A specially-crafted font file could exploit
this overflow and execute arbitrary code with the privileges of the ATS
server process. (3) Finder fails to properly handle malformed
".DS_Store" files, used to store information about directory contents.
By placing a specially-crafted .DS_Store file in a location where it
will be viewed by Finder (e.g. a disk image or shared directory), an
attacker could execute arbitrary code with the privileges of the current
user. (4) WebKit, used by Safari and other applications to process and
render HTML documents, fails to properly handle malformed HTML. A
specially-crafted web page could exploit this vulnerability to execute
arbitrary code with the privileges of the current user. (5) The
Point-to-Point Protocol over Ethernet (PPPoE) subsystem fails to
properly handle specially-crafted PPPoE frames. If PPPoE is used, an
attacker on the local network could exploit this vulnerability and
execute arbitrary code with kernel privileges. PPPoE is not enabled by
default. Additional vulnerabilities exist in third party applications
included in Mac OS X, including perl, Samba, and ClamAV. This security
update also addresses several additional vulnerabilities, including
local-only, denial-of-service, information disclosure, and spoofing
vulnerabilities. An additional denial-of-service vulnerability (not
patched by this Security Update) in the Airport Extreme subsystem was
discovered by the "Month of the Kernel Bugs" project.
```

Status: Apple confirmed, updates available.

Council Site Actions: Three of the responding council sites are using the affected software. One site has already started the process of deploying the patch. Two other sites are relying on Apple's automatic Software Update Facility to deploy the patches.

References:
Posting by Mu Security Detailing PPPoE Vulnerability
http://archives.neohapsis.com/archives/fulldisclosure/2006-11/0504.html
Posting by Month of Kernel Bugs Regarding Airport Extreme DoS
http://projects.info-pull.com/mokb/MOKB-30-11-2006.html
Previous @RISK Newsletter Entry
http://www.sans.org/newsletters/risk/display.php?v=5&i=39#widely3
Apple Security Advisory
http://docs.info.apple.com/article.html?artnum=304829
Mac OS X Home Page
http://www.apple.com/macosx
SecurityFocus BID
http://www.securityfocus.com/bid/21335

(2) HIGH: Adobe AcroPDF ActiveX Control Multiple Vulnerabilities
Affected:
Adobe Reader versions 7.0.0 - 7.0.8
Adobe Acrobat Standard and Professional versions 7.0.0 - 7.0.8

Description: The AcroPDF ActiveX control, included with Adobe Reader and Adobe Acrobat contains multiple vulnerabilities in its "setPageMode()", "setLayoutMode()", "setNamedDest()", and "LoadFile()" methods. A web page that instantiates this control and calls one of these methods could exploit these vulnerabilities and execute arbitrary code with the privileges of the current user. Users can mitigate the impact of this vulnerability by disabling the affected ActiveX control via Microsoft's "kill bit" mechanism for CLSID "{CA8A9780-280D-11CF-A24D-444553540000}".

Status: Adobe confirmed, no updates available.

Council Site Actions: All responding council sites are waiting on additional information from the vendor. Almost all sites rely on the automatic update feature for their clients.

References:
Adobe Security Advisory
http://www.adobe.com/support/security/advisories/apsa06-02.html
FrSIRT Advisory
http://www.frsirt.com/english/advisories/2006/4751
Microsoft Knowledge Base Article detailing the "kill bit" mechanism
http://support.microsoft.com/kb/240797
SecurityFocus BID
http://www.securityfocus.com/bid/21338

(3) MODERATE: Novell Netware Client Print Provider Buffer Overflow
Affected:

Novell Netware Client 4.91 SP0/SP1/SP2

Description: The Novell Netware Client, used to provide access to Netware services (including shared files and printers) for Microsoft Windows systems contains a buffer overflow in its print provider subsystem. By passing overly long arguments to the "EnumPrinters()" or "OpenPrinter()" functions, an attacker could exploit this buffer overflow and execute arbitrary code with SYSTEM privileges. These functions are accessible without authentication via the "spoolss" named pipe.

Status: Novell confirmed, updates available. As a workaround, users are advised to block the TCP ports 139 and 445 at the network perimeter.

Council Site Actions: Only one of the responding council sites is using the affected software and only in one department on a small number of servers. That department is still investigating the impact of the vulnerability.

References:
Zero Day Initiative Advisory
http://www.zerodayinitiative.com/advisories/ZDI-06-043.html
Novell Support Document
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2974765.htm
MSDN Page on Microsoft Remote Procedure Call
http://msdn2.microsoft.com/en-us/library/aa378651.aspx
SecurityFocus BID
http://www.securityfocus.com/bid/21220

(4) MODERATE: Symantec NetBackup PHP Vulnerabilities
Affected:
Symantec Veritas NetBackup PureDisk Remote Office Edition versions 6.0GA, MP1 NB_PDE60_MP1_S01

Description: Symantec NetBackup PureDisk Remote Office Edition, a popular backup solution, was discovered to install a version of PHP with multiple known vulnerabilities. Attackers could exploit these vulnerabilities to execute arbitrary commands with the privileges of the web server process. The vulnerable web server is configured to run with SSL by default, but, depending on configuration, no authentication may be necessary.

Status: Symantec confirmed, updates available.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
Symantec Security Advisory
http://archives.neohapsis.com/archives/bugtraq/2006-11/0574.html
SecurityFocus BID (PHP vulnerabilities)
http://www.securityfocus.com/bid/20879

(5) MODERATE: JBoss DeploymentFileRepository Class Directory Traversal
Affected:
JBoss version 1.0 GA and possibly prior

Description: JBoss, a popular Java-based application server, contains a directory traversal vulnerability. By sending a specially-crafted request to the JBoss management console, an attacker could read, write, or create arbitrary files anywhere in the filesystem where the JBoss server has appropriate privileges. It is possible that this could lead to remote code execution by overwriting or creating files in locations where they will be executed. By default, no authentication is required to access the management console, however, most common configurations require authentication or otherwise limit access.

Status: JBoss confirmed, updates available.

Council Site Actions: Only one responding council site is using the affected software and only on a small number of systems. They will install the Red Hat patches during their next regularly scheduled system maintenance window.

References:
Symantec Security Advisory
http://archives.neohapsis.com/archives/bugtraq/2006-11/0540.html
Posting by Jon Hart
http://archives.neohapsis.com/archives/bugtraq/2006-11/0545.html
SecurityFocus BID
http://www.securityfocus.com/bid/21219

(6) MODERATE: Novell ZENworks Asset Management Multiple Vulnerabilities
Affected:
Novell ZENworks Asset Management version 7.0 SP1 and possibly prior

Description: Novell ZENworks, used to automate IT management, contains multiple vulnerabilities. By sending a specially-crafted request to the Collection client or to the Task or Collection servers, an attacker could exploit these vulnerabilities and execute arbitrary code with the privileges of the vulnerable process. The Collection client runs with SYSTEM privileges on Microsoft Windows systems and root privileges on Unix and Unix-like systems.

Status: Novell confirmed, updates available.

References:
iDefense Security Advisories
http://www.securityfocus.com/archive/1/453236
http://www.securityfocus.com/archive/1/453233
Novell Technical Information Document
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2974824.htm
ZENworks Home Page
http://www.novell.com/products/zenworks/
SecurityFocus BIDs
http://www.securityfocus.com/bid/21400
http://www.securityfocus.com/bid/21395

Other Software

(7) HIGH: 3Com TFTP Server Multiple Buffer Overflows
Affected:
3Com TFTP Server version 2.0.1 and possibly prior
3Com 3CTftpSvc version 2.0.1 and possibly prior

Description: 3Com TFTP server and 3CTftpSvc (the server modified to run as a Microsoft Windows service) contain several remotely exploitable buffer overflows. By sending a specially-crafted TFTP request containing an overly long transport mode or filename to a vulnerable server, an attacker could exploit these vulnerabilities and execute arbitrary code with the privileges of the TFTP server process. Technical details and several exploits are available for these vulnerabilities.

Status: 3Com is aware of the issues, no fix is yet available.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
Posting by Liu Qixu
http://archives.neohapsis.com/archives/bugtraq/2006-11/0526.html
Posting by Kurt Grutzmacher
http://archives.neohapsis.com/archives/fulldisclosure/2006-11/0531.html
Exploits
http://www.securityfocus.com/data/vulnerabilities/exploits/3CTftpSvc_poc.py
http://www.securityfocus.com/data/vulnerabilities/exploits/21301.py
http://www.securityfocus.com/data/vulnerabilities/exploits/3ctftp_overflow.pm
3Com Software Library
http://support.3com.com/software/utilities_for_windows_32_bit.htm
Wikipedia Article on TFTP
http://en.wikipedia.org/wiki/TFTP
SecurityFocus BIDs
http://www.securityfocus.com/bid/21322
http://www.securityfocus.com/bid/21301

(8) MODERATE: Borland idsql32.dll Buffer Overflow
Affected:
Borland idsql32.dll versions 5.1.0.4 and 5.2.0.2 and possibly prior

Description: The idsql32.dll library, used to provide SQL-related services to applications developed with Borland products, contains a buffer overflow. A specially-crafted overlong SQL statement could exploit this buffer overflow and execute arbitrary code with the privileges of the calling application. Note that any application that uses this library is potentially vulnerable.

Status: Borland has not confirmed, no updates available.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any

of the council sites. They reported that no action was necessary.

References:
Secunia Security Advisory
http://archives.neohapsis.com/archives/bugtraq/2006-11/0573.html
RevilloC Mailserver (example vulnerable product)
http://www.revilloc.com/mailserver/default.asp
SecurityFocus BID
http://www.securityfocus.com/bid/21342

Weekly Comprehensive List of Newly Discovered Vulnerabilities

WINDOWS
06.48.1 CVE: Not Available
Platform: Microsoft Office
Title: Microsoft Office HTMLMARQ.OCX Library Denial of Service
Ref: http://www.securityfocus.com/bid/21262

06.48.2 CVE: Not Available
Platform: Other Microsoft Products
Title: Windows Media Player ASX PlayList File Denial of Service
Ref: http://www.securityfocus.com/archive/1/452352

06.48.3 CVE: Not Available
Platform: Other Microsoft Products
Title: MailEnable WebAdmin Unauthorized Access
Ref: http://www.mailenable.com/hotfix/

THIRD PARTY WINDOWS APPLICATIONS
06.48.4 CVE: CVE-2006-6076
Platform: Third Party Windows Apps
Title: BrightStor ARCserve Backup Tape Engine Remote Buffer Overflow
Ref: http://www.frsirt.com/english/advisories/2006/4654

06.48.5 CVE: Not Available
Platform: Third Party Windows Apps
Title: My Firewall Plus Local Privilege Escalation
Ref: http://www.securityfocus.com/bid/21228

06.48.6 CVE: CVE-2006-5965
Platform: Third Party Windows Apps
Title: Passgo SSO Plus Local Insecure Default Directory Permissions
Ref: http://www.securityfocus.com/bid/21244

06.48.7 CVE: Not Available
Platform: Third Party Windows Apps
Title: MailEnable IMAP Service Unspecified Buffer Overflow
Ref: http://www.securityfocus.com/bid/21252

06.48.8 CVE: CVE-2006-4518
Platform: Third Party Windows Apps
Title: Qbik WinGate Remote Denial Of Service
Ref:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=444

06.48.9 CVE: Not Available

Platform: Third Party Windows Apps
Title: 3Com TFTP Transporting Mode Remote Buffer Overflow
Ref: http://www.securityfocus.com/bid/21301

06.48.10 CVE: Not Available
Platform: Third Party Windows Apps
Title: Allied Telesyn AT-TFTP Server Filename Remote Buffer Overflow
Ref: http://www.securityfocus.com/bid/21320

06.48.11 CVE: Not Available
Platform: Third Party Windows Apps
Title: 3Com 3CTftpSvc Filename Remote Buffer Overflow
Ref: http://www.securityfocus.com/bid/21322

06.48.12 CVE: Not Available
Platform: Third Party Windows Apps
Title: Quinnware Quintessential Player Playlist Files Remote Memory Corruption
Ref: http://www.securityfocus.com/bid/21331

MAC OS
06.48.13 CVE: Not Available
Platform: Mac Os
Title: Apple Mac OS X Mach-O Binary Loading Privilege Escalation Vulnerability
Ref: http://projects.info-pull.com/mokb/MOKB-23-11-2006.html

06.48.14 CVE: Not Available
Platform: Mac Os
Title: Apple Mac OS X KQueue Local Denial of Service
Ref:
http://kernelfun.blogspot.com/2006/11/mokb-24-11-2006-mac-os-x-kqueue-local.html

06.48.15 CVE: Not Available
Platform: Mac Os
Title: Apple Mac OS X Mach-O Binary Loading Integer Overflow
Ref: http://www.securityfocus.com/bid/21291

06.48.16 CVE: Not Available
Platform: Mac Os
Title: Apple Mac OS X AppleTalk Local Memory Corruption
Ref: http://www.securityfocus.com/bid/21317

06.48.17 CVE: Not Available
Platform: Mac Os
Title: Apple Safari Password Manager Information Disclosure
Ref:
http://tearesolutions.com/2006/11/how to steal passwords from safaris autofill.html

06.48.18 CVE:
CVE-2006-4396 CVE-2006-4398 CVE-2006-4400 CVE-2006-4401 CVE-2006-4402
CVE-2006-4403 CVE-2006-4404 CVE-2006-4406 CVE-2006-4407 CVE-2006-4408
CVE-2006-4409 CVE-2006-4410 CVE-2006-4411 CVE-2006-4396 CVE-2006-4398
CVE-2006-4400 CVE-2006-4401 CVE-2006-4402 CVE-2006-4403 CVE-2006-4404
CVE-2006-4406 CVE-2006-4407 CVE-2006-4408 CVE-2006-4409 CVE-2006-4410
CVE-2006-4411 CVE-2006-4412

Platform: Mac Os
Title: Apple Mac OS X 2006-007 Multiple Security Vulnerabilities
Ref: http://docs.info.apple.com/article.html?artnum=304829

BSD
06.48.19 CVE: Not Available
Platform: BSD
Title: NetBSD Multiple Local Denial of Service Vulnerabilities
Ref: http://www.securityfocus.com/bid/21327

06.48.20 CVE: Not Available
Platform: BSD
Title: NetBSD Kernel Multiple Local Information Disclosure Vulnerabilities
Ref: http://www.securityfocus.com/bid/21328

CROSS PLATFORM
06.48.21 CVE: Not Available
Platform: Cross Platform
Title: Net-SNMP Unspecified Malformed TCP Packet Remote Denial Of Service
Ref: http://www.securityfocus.com/bid/21256

06.48.22 CVE: Not Available
Platform: Cross Platform
Title: Haru Free PDF Library HPDF_Page_Circle Buffer Overflow Vulnerability
Ref: http://sourceforge.net/tracker/index.php?func=detail&aid=1597538&group_id=83044&atid=568129

06.48.23 CVE: CVE-2006-6077
Platform: Cross Platform
Title: Mozilla Firefox 2 Password Manager Information Disclosure
Ref: https://bugzilla.mozilla.org/show_bug.cgi?id=360493

06.48.24 CVE: Not Available
Platform: Cross Platform
Title: Business Objects Crystal Reports XI Professional File Handling Buffer Overflow
Ref: http://www.securityfocus.com/bid/21261

06.48.25 CVE: Not Available
Platform: Cross Platform
Title: JBoss Java Class DeploymentFileRepository Directory Traversal
Ref: http://www.securityfocus.com/bid/21219

06.48.26 CVE: CVE-2006-5869
Platform: Cross Platform
Title: PSToText Filename Handling Shell Command Execution Vulnerability
Ref: http://www.securityfocus.com/bid/21299

06.48.27 CVE: Not Available
Platform: Cross Platform
Title: CRYPTOCard CRYPTO-Server Local Information Disclosure

Ref: http://www.securityfocus.com/bid/21305

06.48.28 CVE: CVE-2006-6169
Platform: Cross Platform
Title: GnuPG Remote Buffer Overflow
Ref: https://bugs.g10code.com/gnupg/issue728

06.48.29 CVE: Not Available
Platform: Cross Platform
Title: GNotebook Local Information Disclosure
Ref: http://www.securityfocus.com/bid/21307

06.48.30 CVE: Not Available
Platform: Cross Platform
Title: ProFTPD MOD_TLS Remote Buffer Overflow
Ref: http://www.securityfocus.com/bid/21326

WEB APPLICATIONS
06.48.31 CVE: CVE-2006-6087
Platform: Web Application - Cross Site Scripting
Title: My Little Weblog Weblog.php Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/21238

06.48.32 CVE: CVE-2006-6091
Platform: Web Application - Cross Site Scripting
Title: GrimBB Multiple Unspecified Cross-Site Scripting Vulnerabilities
Ref:
http://sourceforge.net/project/shownotes.php?release_id=465519&group_id=182536

06.48.33 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: InverseFlow Help Desk Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452397

06.48.34 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: Simple PHP Gallery System SP_Index.PHP Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/21278

06.48.35 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: MMGallery Thumbs.PHP Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/21281

06.48.36 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: Expinion.net iNews Publisher Articles.ASP Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/bid/21296

06.48.37 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: TDiary Unspecified Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/21321

06.48.38 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: Wordpress Index.PHP Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/21318

06.48.39 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: b2evolution Error Pages Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452895

06.48.40 CVE: Not Available
Platform: Web Application - SQL Injection
Title: FipsCMS Index.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21258

06.48.41 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Neocrome Land Down Under Profile.Inc.PHP SQL Injection
Ref: http://www.securityfocus.com/archive/1/452259

06.48.42 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Seditio Users.Profile.Inc.PHP SQL Injection
Ref: http://neocrome.net/page.php?al=avselect

06.48.43 CVE: Not Available
Platform: Web Application - SQL Injection
Title: SoftAcid Reciprocal Link Exchange Lite SQL Injection
Ref: http://www.securityfocus.com/bid/21239

06.48.44 CVE: Not Available
Platform: Web Application - SQL Injection
Title: FipsForum Default2.ASP SQL Injection Vulnerability
Ref: http://www.securityfocus.com/bid/21253

06.48.45 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Recipes Complete Website SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21270

06.48.46 CVE: Not Available
Platform: Web Application - SQL Injection
Title: JiRo's FAQ Manager Login.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21271

06.48.47 CVE: Not Available
Platform: Web Application - SQL Injection
Title: MidiCart ASP Item_Show.ASP ID2006quant Parameter SQL Injection
Ref: http://www.securityfocus.com/bid/21273

06.48.48 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Wallpaper Complete Website Wallpaper.PHP SQL Injection
Ref: http://www.securityfocus.com/bid/21274

06.48.49 CVE: Not Available

Platform: Web Application - SQL Injection
Title: PHP-Nuke News Module Index.PHP SQL Injection
Ref: http://www.securityfocus.com/bid/21277

06.48.50 CVE: Not Available
Platform: Web Application - SQL Injection
Title: ASP ListPics Listpics.ASP SQL Injection
Ref: http://www.securityfocus.com/archive/1/452569

06.48.51 CVE: Not Available
Platform: Web Application - SQL Injection
Title: fipsShop Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21289

06.48.52 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Nivisec Hacks List HACK_ID SQL Injection
Ref: http://www.securityfocus.com/bid/21290

06.48.53 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Liberum Help Desk DETAILS.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21292

06.48.54 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Clickblog Displaycalendar.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21310

06.48.55 CVE: Not Available
Platform: Web Application - SQL Injection
Title: ClickContact Default.ASP Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452825

06.48.56 CVE: Not Available
Platform: Web Application - SQL Injection
Title: uPhotoGallery Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452827

06.48.57 CVE: Not Available
Platform: Web Application - SQL Injection
Title: WarHound General Shopping Cart Item.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21324

06.48.58 CVE: Not Available
Platform: Web Application
Title: FipsGallery Index1.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21254

06.48.59 CVE: Not Available
Platform: Web Application
Title: E-Ark Ark_Inc.PHP Remote File Include
Ref: http://www.securityfocus.com/bid/21224

06.48.60 CVE: CVE-2006-6083, CVE-2006-6082
Platform: Web Application
Title: Creascripts Creadirectory Multiple Input Validation

Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452241

06.48.61 CVE: Not Available
Platform: Web Application
Title: VMware VirtualCenter SSL Session Man In The Middle
Ref: http://www.securityfocus.com/bid/21231

06.48.62 CVE: Not Available
Platform: Web Application
Title: Cutenews Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21233

06.48.63 CVE: Not Available
Platform: Web Application
Title: Deskpro Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21248

06.48.64 CVE: CVE-2006-3340
Platform: Web Application
Title: Pearl Forums for Mambo Multiple Remote File Include
Vulnerabilities
Ref: http://www.securityfocus.com/bid/21249

06.48.65 CVE: Not Available
Platform: Web Application
Title: Messagerie Locale Page Remote File Include Vulnerability
Ref: http://www.securityfocus.com/bid/21267

06.48.66 CVE: Not Available
Platform: Web Application
Title: PEGames Remote File Include
Ref: http://www.securityfocus.com/bid/21266

06.48.67 CVE: Not Available
Platform: Web Application
Title: Woltlab Burning Board WBB_UserID SQL Injection
Ref: http://www.securityfocus.com/bid/21265

06.48.68 CVE: Not Available
Platform: Web Application
Title: Owllib OWLLIB_ROOT Remote File Include
Ref: http://www.securityfocus.com/bid/21268

06.48.69 CVE: Not Available
Platform: Web Application
Title: HIOXS Star Rating System Addcode.PHP Remote File Include
Ref: http://www.securityfocus.com/bid/21280

06.48.70 CVE: Not Available
Platform: Web Application
Title: Fixit iDMS Pro Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21282

06.48.71 CVE: Not Available
Platform: Web Application
Title: Cahier De Texte Telecharger.PHP Directory Traversal

Ref: http://www.securityfocus.com/archive/1/452600

06.48.72 CVE: Not Available
Platform: Web Application
Title: nukeai Util.PHP Remote Code Execution
Ref: http://www.securityfocus.com/bid/21284

06.48.73 CVE: Not Available
Platform: Web Application
Title: SIAP CMS Login.ASP SQL Injection
Ref: http://www.securityfocus.com/archive/1/452642

06.48.74 CVE: Not Available
Platform: Web Application
Title: WebHost Manager Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/bid/21288

06.48.75 CVE: Not Available
Platform: Web Application
Title: Sysinfo Kampus Multiple Remote File Include Vulnerabilities
Ref: http://www.securityfocus.com/bid/21294

06.48.76 CVE: CVE-2006-6163
Platform: Web Application
Title: TikiWiki PageAlias HTML Injection
Ref: http://www.securityfocus.com/bid/21297

06.48.77 CVE: Not Available
Platform: Web Application
Title: Mambo Jambook Entry Field HTML Injection
Ref: http://www.securityfocus.com/bid/21298

06.48.78 CVE: Not Available
Platform: Web Application
Title: MBoard Orig_ID Input Validation
Ref: http://www.securityfocus.com/bid/21304

06.48.79 CVE: Not Available
Platform: Web Application
Title: Asp-Nuke Community Cookie Privilege Escalation
Ref: http://www.securityfocus.com/bid/21309

06.48.80 CVE: Not Available
Platform: Web Application
Title: Click Gallery Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21311

06.48.81 CVE: Not Available
Platform: Web Application
Title: Exhibit Engine Styles.PHP Remote File Include
Ref: http://www.securityfocus.com/bid/21313

06.48.82 CVE: Not Available
Platform: Web Application
Title: Mambo Flyspray Startdown.PHP Information Disclosure
Ref: http://www.securityfocus.com/bid/21315

06.48.83 CVE: Not Available
Platform: Web Application
Title: Evolve Shopping Cart products.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21323

06.48.84 CVE: Not Available
Platform: Web Application
Title: b2evolution Import-MT.PHP Remote File Include Vulnerability
Ref: http://www.securityfocus.com/bid/21332

06.48.85 CVE: CVE-2006-6125
Platform: Network Device
Title: NetGear WG311v1 Wireless Driver SSID Heap Buffer Overflow
Ref: http://projects.info-pull.com/mokb/MOKB-22-11-2006.html

06.48.86 CVE: Not Available
Platform: Network Device
Title: GNU Radius SQLLog Remote Format String
Ref: http://www.securityfocus.com/archive/1/452789

Thank you,
Information Security Operations Center (ISOC)
isoc@state.co.us
(303) 866-3465

E-MAIL NOTICE: This e-mail message (and any attachments) contains information belonging to the sender, which is confidential and legally privileged. If you are not the intended recipient, you are hereby notified that any disclosure, coping or distribution of this information or any action taken in reliance on the information within this email is strictly prohibited. If you have received this e-mail in error, please notify the sender and then delete the message (and any attachments) from your computer. Thank You.
*"Information Security - Working Together to Make **IT** happen"*