

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[WinArpd v1.0b8](#) - Download WinArpd executable by filling our download form. Size: 55KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winarpd.exe.zip>

This Week in Review

Lawsuit against NSA. Cloud computing becoming a hot issue. The perception on cybercrime. New law expands scope of cybercrime.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.

(503) 524 5758 or sales@netvigilance.com

Top Security News Stories this Week

• EFF files surveillance lawsuit against NSA, Bush, Cheney

September 18, 2008 (IDG News Service) WASHINGTON -- The Electronic Frontier Foundation filed a lawsuit against the U.S. National Security Agency, President George W. Bush, Vice President Dick Cheney and other government officials, alleging that an NSA electronic surveillance program continues to illegally spy on U.S. residents.

The lawsuit alleges that the NSA installed equipment to conduct mass surveillance at AT&T telecommunications facilities in San Francisco, Atlanta, Seattle, Los Angeles, San Diego, San Jose, and Bridgeton, Mo. "We allege a nationwide network of such NSA vacuum-cleaner surveillance facilities that would indiscriminately collect communications of all of the people who use AT&T's network," said Kevin Bankston, senior staff attorney at the EFF.

The White House and the NSA didn't immediately respond to requests for comment on the lawsuit. Bush administration officials have long defended the program as essential for fighting terrorism.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115101&source=rss_topic1

• Cloud computing could prompt government action

September 12, 2008 (IDG News Service) Cloud computing will soon become a hot topic in Washington, D.C., with policy makers debating issues such as the privacy and security of data in the cloud, a panel of tech experts said Friday.

Among the major policy issues to be worked out: Who owns the data that consumers store on the network? Should law enforcement agencies have easier access to personal information in the cloud than data on a personal computer? Do government procurement regulations need to change to allow agencies to embrace cloud computing?

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114587&source=rss_topic1

• Study: Companies increasingly wary of cybercrime

Cybercrime is perceived as a major business risk to organizations -- with risks to intellectual property and sensitive corporate information the main concern.

Respondents also indicated that data breaches could go unnoticed, and that malware tucked into their business data is a greater issue than virus infections. Results also showed that many companies do not have a Web 2.0 policy in place.

Yuval Ben-Itzhak, chief technology officer of Finjan, said: "It is indicative of the domination of criminal gangs in the malware and security attack business these days.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Study-Companies-increasingly-wary-of-cybercrime/article/118129/>

• Report: 60 percent of businesses hit by cybercrime

A recent Department of Justice survey indicated that nearly 60 percent of American businesses have detected one or more cyberattacks.

The survey, dubbed the National Computer Security Survey (NCSS), also revealed that 11 percent of the respondents detected actual losses from cyberthefts and that 24 percent had identified computer-related security incidents.

Though the NCSS reported that computer viruses were the most common type of cyberattack -- detected by 52 percent of reporting businesses in 2005 -- malware that steals corporate data is a bigger risk today, Ophir Shalitin, director of marketing for Finjan told SCMagazineUS.com on Thursday.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Report-60-percent-of-businesses-hit-by-cybercrime/article/118195/>

New Vulnerabilities Tested in SecureScout

• 18084 VMware Server, ActiveX control unspecified vulnerability (CVE-2008-3691) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Server before 1.0.7 build 108231, has unknown impact and remote attack vectors.

The issue is fixed in VMware Server 1.0.7.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

- * BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues. <http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>
- * FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues. <http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>
- * CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708

<http://secunia.com/advisories/31708>

* SECUNIA: 31709

<http://secunia.com/advisories/31709>

* SECUNIA: 31710

<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3691 (cve.mitre.org, nvd.nist.gov)

• 18086 VMware Server, ActiveX control unspecified vulnerability (CVE-2008-3692) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Server before 1.0.7 build 108231, has unknown impact and remote attack vectors.

The issue is fixed in VMware Server 1.0.7.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708

<http://secunia.com/advisories/31708>

* SECUNIA: 31709

<http://secunia.com/advisories/31709>

* SECUNIA: 31710

<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3692 (cve.mitre.org, nvd.nist.gov)

• 18088 VMware Server, ActiveX control unspecified vulnerability (CVE-2008-3693) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Server before 1.0.7 build 108231, has unknown impact and remote attack vectors.

The issue is fixed in VMware Server 1.0.7.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708

<http://secunia.com/advisories/31708>

* SECUNIA: 31709

<http://secunia.com/advisories/31709>

* SECUNIA: 31710

<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3693 (cve.mitre.org, nvd.nist.gov)

• 18090 VMware Server, ActiveX control unspecified vulnerability (CVE-2008-3694) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Server before 1.0.7 build 108231, has unknown impact and remote attack vectors.

The issue is fixed in VMware Server 1.0.7.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE,

VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708

<http://secunia.com/advisories/31708>

* SECUNIA: 31709

<http://secunia.com/advisories/31709>

* SECUNIA: 31710

<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3694 (cve.mitre.org, nvd.nist.gov)

• 18092 VMware Server, ActiveX control unspecified vulnerability (CVE-2008-3695) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Server before 1.0.7 build 108231, has unknown impact and remote attack vectors.

The issue is fixed in VMware Server 1.0.7.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708
<http://secunia.com/advisories/31708>
* SECUNIA: 31709
<http://secunia.com/advisories/31709>
* SECUNIA: 31710
<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3695 (cve.mitre.org, nvd.nist.gov)

• 18094 VMware Server, ActiveX control unspecified vulnerability (CVE-2008-3696) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Server before 1.0.7 build 108231, has unknown impact and remote attack vectors.

The issue is fixed in VMware Server 1.0.7.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.
<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>
* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.
<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>
* CONFIRM:
http://www.vmware.com/support/ace/doc/releasenotes_ace.html
* CONFIRM:
http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html
* CONFIRM:
http://www.vmware.com/support/player/doc/releasenotes_player.html
* CONFIRM:
http://www.vmware.com/support/player2/doc/releasenotes_player2.html
* CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html
* CONFIRM:
http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html
* BID: 30934
<http://www.securityfocus.com/bid/30934>
* FRSIRT: ADV-2008-2466
<http://www.frst.com/english/advisories/2008/2466>
* SECUNIA: 31707
<http://secunia.com/advisories/31707>
* SECUNIA: 31708
<http://secunia.com/advisories/31708>
* SECUNIA: 31709
<http://secunia.com/advisories/31709>
* SECUNIA: 31710
<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3696 (cve.mitre.org, nvd.nist.gov)

• 18096 VMware Server, OpenProcess function unspecified vulnerability (Remote File Checking)

Unspecified vulnerability in the OpenProcess function in VMware Server before 1.0.7 build 108231, on Windows allows local host OS users to gain privileges on the host OS via unknown vectors.

The issue is fixed in VMware Server 1.0.7.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30936

<http://www.securityfocus.com/bid/30936>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

CVE Reference:

CVE-2008-3698 (cve.mitre.org, nvd.nist.gov)

• 18125 QuickTime Indeo v5 codec crafted movie file, application termination and arbitrary code execution Vulnerability (Remote File Checking)

An uninitialized memory access issue exists in the third-party Indeo v5 codec for QuickTime, which does not ship with QuickTime. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by not rendering content encoded with any version of the Indeo codec. This issue does not affect systems running Mac OS X.

The issue has been fixed in version 7.5.5.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack** Risk: **High**

References:

* BUGTRAQ:

<http://www.securityfocus.com/archive/1/archive/1/496358/100/0/threaded>

* MISC:

<http://www.ngssoftware.com/advisories/critical-vulnerability-in-apple-quicktimes-indeo-codec/>

* CONFIRM:

<http://support.apple.com/kb/HT3027>

* APPLE:

<http://lists.apple.com/archives/security-announce//2008/Sep/msg00000.html>

* BID:

<http://www.securityfocus.com/bid/31086>

* SECTRACK:

<http://securitytracker.com/id?1020841>

* SECUNIA:

<http://secunia.com/advisories/31821>

CVE Reference:

CVE-2008-3615 (cve.mitre.org, nvd.nist.gov)

• 18126 QuickTime Indeo v3.2 codec crafted movie file, application termination and arbitrary code execution Vulnerability (Remote File Checking)

A stack buffer overflow exists in the third-party Indeo v3.2 codec for QuickTime. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by not rendering content encoded with any version of the Indeo codec. This issue does not affect systems running Mac OS X.

The issue has been fixed in version 7.5.5.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack** Risk: **High**

References:

- * BUGTRAQ: 20080909 ZDI-08-057: Apple QuickTime IV32 Codec Parsing Stack Overflow Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/496201/100/0/threaded>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-057/>
- * CONFIRM:
<http://support.apple.com/kb/HT3027>
- * APPLE: APPLE-SA-2008-09-09
<http://lists.apple.com/archives/security-announce//2008/Sep/msg00000.html>
- * BID: 31086
<http://www.securityfocus.com/bid/31086>
- * SECTRACK: 1020841
<http://securitytracker.com/id?1020841>

CVE Reference:

CVE-2008-3635 (cve.mitre.org, nvd.nist.gov)

• 18127 QuickTime maliciously crafted QTVR movie file, application termination and arbitrary code execution Vulnerability (CVE-2008-3624) (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of panorama atoms in QTVR (QuickTime Virtual Reality) movie files. Viewing a maliciously crafted QTVR file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.5.5.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack** Risk: **High**

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3027>
- * APPLE: APPLE-SA-2008-09-09
<http://lists.apple.com/archives/security-announce//2008/Sep/msg00000.html>
- * BID:
<http://www.securityfocus.com/bid/31086>
- * SECTRACK:
<http://securitytracker.com/id?1020841>
- * SECUNIA:
<http://secunia.com/advisories/31821>

CVE Reference:

CVE-2008-3624 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-4110 Microsoft CVSS 2.0 Score = 10.0

Buffer overflow in the SQLVDIRLib.SQLVDirControl ActiveX control in Tools\Binn\sqlvdir.dll in Microsoft SQL Server 2000 (aka SQL Server 8.0) allows remote attackers to cause a denial of service (browser crash) or possibly execute arbitrary code via a long URL in the second argument to the Connect method. NOTE: this issue might only be exploitable in limited browser configurations.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

- XF: <http://xforce.iss.net/xforce/xfdb/45186>
- BID: <http://www.securityfocus.com/bid/31129>
- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496232/100/0/threaded>

CVE Reference: [CVE-2008-4110](http://cve.mitre.org)

• CVE-2008-4114 Microsoft CVSS 2.0 Score = 7.1

srv.sys in Microsoft Windows Vista SP1 allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via an SMB WRITE_ANDX packet with an offset that is inconsistent with the

packet size, as demonstrated by a request to the \PIPE\lsarpc named pipe.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

XF: <http://xforce.iss.net/xforce/xfdb/45146>

MISC: http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm

SECTRAK: <http://www.securitytracker.com/id?1020887>

BID: <http://www.securityfocus.com/bid/31179>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496354/100/0/threaded>

MISC: http://www.reversemode.com/index.php?option=com_content&task=view&id=54&Itemid=1

MILWORM: <http://www.milw0rm.com/exploits/6463>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2583>

SECUNIA: <http://secunia.com/advisories/31883>

CVE Reference: [CVE-2008-4114](#)

• **CVE-2008-4127 Microsoft CVSS 2.0 Score = 4.3**

Mshhtml.dll in Microsoft Internet Explorer 7 Gold 7.0.5730 and 8 Beta 8.0.6001 on Windows XP SP2 allows remote attackers to cause a denial of service (failure of subsequent image rendering) via a crafted PNG file, related to an infinite loop in the CDwnTaskExec::ThreadExec function.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

XF: <http://xforce.iss.net/xforce/xfdb/45225>

BID: <http://www.securityfocus.com/bid/31215>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496483/100/0/threaded>

CVE Reference: [CVE-2008-4127](#)

• **CVE-2008-4097 MySQL CVSS 2.0 Score = 4.6**

MySQL 5.0.51a allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are associated with symlinks within pathnames for subdirectories of the MySQL home data directory, which are followed when tables are created in the future. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-2079.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

MLIST: <http://www.openwall.com/lists/oss-security/2008/09/16/3>

MLIST: <http://www.openwall.com/lists/oss-security/2008/09/09/20>

CONFIRM: <http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=480292#25>

CVE Reference: [CVE-2008-4097](#)

• **CVE-2008-4098 MySQL CVSS 2.0 Score = 4.6**

MySQL before 5.0.67 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL home data directory. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4097.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: <http://bugs.mysql.com/bug.php?id=32167>

MLIST: <http://www.openwall.com/lists/oss-security/2008/09/16/3>

MLIST: <http://www.openwall.com/lists/oss-security/2008/09/09/20>

CVE Reference: [CVE-2008-4098](#)

• **CVE-2008-4111 IBM CVSS 2.0 Score = 9.3**

Unspecified vulnerability in Servlet Engine/Web Container in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.19, when the FileServing feature is enabled, has unknown impact and attack vectors.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

XF: <http://xforce.iss.net/xforce/xfdb/45122>

BID: <http://www.securityfocus.com/bid/31186>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2566>

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1PK64302>

SECUNIA: <http://secunia.com/advisories/31892>

CVE Reference: [CVE-2008-4111](#)

• **CVE-2008-4128 Cisco CVSS 2.0 Score = 9.3**

Multiple cross-site request forgery (CSRF) vulnerabilities in the HTTP Administration component in Cisco IOS 12.4 on the 871 Integrated Services Router allow remote attackers to execute arbitrary commands via (1) a certain "show privilege" command to the /level/15/exec/- URI, and (2) a certain "alias exec" command to the /level/15/exec/-/configure/http URI. NOTE: some of these details are obtained from third party information. Additional details: <http://jbrownsec.blogspot.com/2008/09/cisco-0day-released.html>

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

XF: <http://xforce.iss.net/xforce/xfdb/45226>

BID: <http://www.securityfocus.com/bid/31218>

MILWORM: <http://www.milw0rm.com/exploits/6477>

MILWORM: <http://www.milw0rm.com/exploits/6476>

MISC: <http://jbrownsec.blogspot.com/2008/09/cisco-0day-released.html>

CVE Reference: [CVE-2008-4128](#)

• **CVE-2008-3616 Apple CVSS 2.0 Score = 10.0**

Multiple integer overflows in the SearchKit API in Apple Mac OS X 10.4.11 and 10.5 through 10.5.4 allow context-dependent attackers to cause a denial of service (application crash) or execute arbitrary code via vectors associated with "passing untrusted input" to unspecified API functions.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

BID: <http://www.securityfocus.com/bid/31189>

APPLE: <http://lists.apple.com/archives/security-announce//2008/Sep/msg00005.html>

XF: <http://xforce.iss.net/xforce/xfdb/45172>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2584>

SECTRACK: <http://securitytracker.com/id?1020880>

SECUNIA: <http://secunia.com/advisories/31882>

CVE Reference: [CVE-2008-3616](#)

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. <http://www.infosyssec.org/infosyssec/>

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com

About SecureScout

SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.

SecureScout is a trademark of NexantiS Corporation.

netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:

Customers in America and Northern Europe contact us at info@netVigilance.com

Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net