netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 23

June 6, 2008

Table of Contents

Product Focus

Apache Chunked Vulnerability Scanner – The S4 Apache Chunked Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Apache Chunked Encoding buffer overflow.

CTO Jesper Jurcenoks of netVigilance is speaker at the HP Technology Forum & Expo 2008 in Las Vegas June 19, see
http://www.netvigilance.com/events

This Week in Review

Canadian businesses need to get their act together. Elegant whaling attack in the wild. Will deep packet inspection be part of a good security strategy in the future. Chinese officials accused of breaking into US systems.

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

- **Businesses too lax with data, says privacy commissioner**

Identity theft feared as watchdog cites 'epidemic' of breaches

So many businesses are playing fast and loose with Canadians' personal information that data breaches have become virtually "epidemic," federal Privacy Commissioner Jennifer Stoddart says.

In her annual report released yesterday, Stoddart said that over the past few years, hundreds of thousands of Canadians have been affected by data breaches, with financial institutions being the worst culprits.

"Data breaches have been reported or noted for years, but they are kind of growing into an ... epidemic proportion not only in Canada but elsewhere," the commissioner told the Toronto Star yesterday.

The start

Full Story :
http://www.thestar.com/News/Canada/article/436591

❖ 'Whaling' Scam Targets Execs Via Tax Court Ruse

A new whaling scam -- that's a phishing scam that targets big game -- using a supposed U.S. Tax Court notification as bait has reeled in about 600 victims so far, according to Internet security firm SecureWorks.

The phishing e-mails appear to come from a Chinese hacker also believed to be responsible for a number of attacks earlier this year targeting C-level executives. The previous attacks have purported to be notifications of legal action from a federal court or the Internal Revenue Service and included a link in the body of the e-mail to download documents.
The current attack supposedly is from the U.S. Tax Court, and downloading the phony document actually installs spyware masquerading as an Adobe Acrobat ActiveX control.

Redmondmag.com

Full Story :
http://redmondmag.com/news/article.asp?EditorialsID=9926

❖ LSI Supports Founding of Organization to Increase Awareness of Deep Packet Inspection

dPacket.org to serve as global resource for all topics related to deep packet Inspection.
LSI Corporation
(NYSE: LSI) today announced it has partnered with nine other companies to found an organization focused on deep packet inspection (DPI). The mission of dPacket.org is to become the premier resource for information, expert discussion and collaboration on DPI. An increased awareness of the need for DPI, corresponding solutions to fill that need and broad community involvement will be the result of the efforts of this group.

Prnewswire

Full Story :

http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=ind_focus.story&STORY=/www/story/06-03-2008/0004825430&EDATE=TUE+Jun+03+2008,+09:33+AM

- **Potential security breach by China?**

A government laptop used by Secretary of Commerce Carlos Gutierrez may have been breached during a visit to Bejing last December.
U.S. authorities are investigating whether Chinese officials secretly copied information from Gutierrez's laptop and then tried to hack into Commerce Department computers, according to published reports.
The laptop was left unattended during the trip, and it is believed the content was copied at that time, reports said.
Since December, the U.S. Computer Emergency Readiness Team (US-CERT) has been called in to work on Commerce Department computers at least eight times; three of those calls were allegedly in response to possible data security break-ins.

scmagazine

Full Story :
http://www.scmagazineus.com/Potential-security-breach-by-China/article/110790/

New Vulnerabilities Tested in SecureScout

- **16757 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (oct-2005/AS02)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Containers for J2EE component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html
* CERT: TA05-292A
http://www.us-cert.gov/cas/techalerts/TA05-292A.html
* CERT-VN: VU#210524
http://www.kb.cert.org/vuls/id/210524
* CERT-VN: VU#376756
http://www.kb.cert.org/vuls/id/376756
* CERT-VN: VU#512716
http://www.kb.cert.org/vuls/id/512716
* BID: 15134
http://www.securityfocus.com/bid/15134
* SECUNIA: 17250
http://secunia.com/advisories/17250

CVE Reference:

CVE-2005-3449 (cve.mitre.org, nvd.nist.gov)

- **16919 Cisco IOS Secure Shell Denial of Service Vulnerabilities (cisco-sa-20080521-ssh)**

Secure shell (SSH) was developed as a secure replacement for the telnet, ftp, rlogin, rsh, and rcp protocols, which allow for the remote access of devices. The main difference between SSH and older protocols is that SSH provides strong authentication, guarantees confidentiality, and uses encrypted transactions.

The server side of the SSH implementation in Cisco IOS contains multiple vulnerabilities that allow an unauthenticated user to generate a spurious memory access or, in certain cases, reload the device. If the attacker is able to reload the device, these vulnerabilities could be repeatedly exploited to cause an extended Denial of Service (DoS) condition.

A device with the SSH server enabled is vulnerable.

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

References:

* CISCO: cisco-sa-20080521-ssh
http://www.cisco.com/en/US/products/products_security_advisory09186a008099567f.shtml
* XF: cisco-ios-ssh-multiple-dos(42563)
http://xforce.iss.net/xforce/xfdb/42563
* BID: 29314
http://www.securityfocus.com/bid/29314
* SECTRACK: 1020073
http://securitytracker.com/id?1020073

CVE Reference:

CVE-2008-1159 (cve.mitre.org, nvd.nist.gov)

- **16943 OpenSSL unknown message types Denial of Service Vulnerability**

OpenSSL 0.9.6 before 0.9.6d does not properly handle unknown message types, which allows remote attackers to cause a denial of service (infinite loop), as demonstrated using the Codenomicon TLS Test Tool.

OpenSSL 0.9.6d fixes the issue.

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

References:

* BUGTRAQ: 20040317 Re: New OpenSSL releases fix denial of service attacks [17 March 2004]

http://marc.theaimsgroup.com/?l=bugtraq&m=107955049331965&w=2
* CISCO: 20040317 Cisco OpenSSL Implementation Vulnerability
http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml
* DEBIAN: DSA-465
http://www.debian.org/security/2004/dsa-465
* FEDORA: FEDORA-2004-095
http://fedoranews.org/updates/FEDORA-2004-095.shtml
* GENTOO: GLSA-200403-03
http://security.gentoo.org/glsa/glsa-200403-03.xml
* REDHAT: RHSA-2004:119
http://rhn.redhat.com/errata/RHSA-2004-119.html
* REDHAT: RHSA-2004:120
http://www.redhat.com/support/errata/RHSA-2004-120.html
* REDHAT: RHSA-2004:121
http://www.redhat.com/support/errata/RHSA-2004-121.html
* REDHAT: RHSA-2004:139
http://www.redhat.com/support/errata/RHSA-2004-139.html
* SCO: SCOSA-2004.10
ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2004.10/SCOSA-2004.10.txt
* SGI: 20040304-01-U
ftp://patches.sgi.com/support/free/security/advisories/20040304-01-U.asc
* SUNALERT: 57524
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57524
* TRUSTIX: 2004-0012
http://www.trustix.org/errata/2004/0012
* BUGTRAQ: 20040508 [FLSA-2004:1395] Updated OpenSSL resolves security vulnerability
http://marc.theaimsgroup.com/?l=bugtraq&m=108403850228012&w=2
* CERT: TA04-078A
http://www.us-cert.gov/cas/techalerts/TA04-078A.html
* CERT-VN: VU#465542
http://www.kb.cert.org/vuls/id/465542
* BID: 9899
http://www.securityfocus.com/bid/9899
* OVAL: oval:org.mitre.oval:def:871
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:871
* OVAL: oval:org.mitre.oval:def:902
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:902
* SECUNIA: 11139
http://secunia.com/advisories/11139
* XF: openssl-tls-dos(15509)
http://xforce.iss.net/xforce/xfdb/15509

CVE Reference:

CVE-2004-0081 (cve.mitre.org, nvd.nist.gov)

- **17790 PHP GENERATE_SEED macro predictable rand() and mt_rand() return values Vulnerability**

The GENERATE_SEED macro in PHP, when running on 32-bit systems, performs a multiplication using values that can produce a zero seed in rare circumstances, which allows context-dependent attackers to predict subsequent values of the rand and mt_rand functions and possibly bypass protection mechanisms that rely on an

unknown initial seed.

The vulnerability has been confirmed in version 4.x up to 4.4.8 included and 5.x up to 5.2.5 included.

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

References:

* BUGTRAQ: 20080506 Advisory SE-2008-02: PHP GENERATE_SEED() Weak Random Number Seed Vulnerability
http://www.securityfocus.com/archive/1/archive/1/491683/100/0/threaded
* FULLDISC: 20080506 Advisory SE-2008-02: PHP GENERATE_SEED() Weak Random Number Seed Vulnerability
http://archives.neohapsis.com/archives/fulldisclosure/2008-05/0103.html
* MISC:
http://www.sektioneins.de/advisories/SE-2008-02.txt
* XF: php-generateseed-weak-security(42226)
http://xforce.iss.net/xforce/xfdb/42226
* XF: php-generateseed-security-bypass(42284)
http://xforce.iss.net/xforce/xfdb/42284

CVE Reference:

CVE-2008-2107 (cve.mitre.org, nvd.nist.gov)

• 17791 PHP GENERATE_SEED macro predictable rand() and mt_rand() return values Vulnerability (64-bit systems)

The GENERATE_SEED macro in PHP, when running on 64-bit systems, performs a multiplication that generates a portion of zero bits during conversion due to insufficient precision, which produces 24 bits of entropy and simplifies brute force attacks against protection mechanisms that use the rand and mt_rand functions.

The vulnerability has been confirmed in version 4.x up to 4.4.8 included and 5.x up to 5.2.5 included.

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

References:

* BUGTRAQ: 20080506 Advisory SE-2008-02: PHP GENERATE_SEED() Weak Random Number Seed Vulnerability
http://www.securityfocus.com/archive/1/archive/1/491683/100/0/threaded
* FULLDISC: 20080506 Advisory SE-2008-02: PHP GENERATE_SEED() Weak Random Number Seed Vulnerability
http://archives.neohapsis.com/archives/fulldisclosure/2008-05/0103.html
* MISC:
http://www.sektioneins.de/advisories/SE-2008-02.txt
* XF: php-generateseed-weak-security(42226)
http://xforce.iss.net/xforce/xfdb/42226

CVE Reference:

CVE-2008-2108 (cve.mitre.org, nvd.nist.gov)

- **17792 PHP Tidy extension arbitrary code execution Vulnerability**

Multiple buffer overflows in libtidy, as used in the Tidy extension for PHP 5.2.3 and possibly other products, allow context-dependent attackers to execute arbitrary code via a long second argument to the tidy_parse_string function or an unspecified vector to the tidy_repair_string function. NOTE: this might only be an issue in environments where vsnprintf is implemented as a wrapper for vsprintf.

The vulnerability has been confirmed in version 5.x up to 5.2.3 included.

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

References:

* MILW0RM: 4080
http://www.milw0rm.com/exploits/4080
* SECUNIA: 25735
http://secunia.com/advisories/25735
* XF: php-tidy-parsestring-bo(34931)
http://xforce.iss.net/xforce/xfdb/34931

CVE Reference:

CVE-2007-3294 (cve.mitre.org, nvd.nist.gov)

- **17793 PHP mSQL extension arbitrary code execution Vulnerability**

Buffer overflow in the mSQL extension in PHP 5.2.3 allows context-dependent attackers to execute arbitrary code via a long first argument to the msql_connect function.

The vulnerability has been confirmed in version 5.x up to 5.2.3 included.

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

References:

* BUGTRAQ: 20070805 PHP mSQL (msql_connect) Buffer Overflow PoC
http://www.securityfocus.com/archive/1/archive/1/475660/100/0/threaded
* MILW0RM: 4260
http://www.milw0rm.com/exploits/4260
* BID: 25213
http://www.securityfocus.com/bid/25213
* XF: php-msql-connect-bo(35830)
http://xforce.iss.net/xforce/xfdb/35830

CVE Reference:

CVE-2007-4255 (cve.mitre.org, nvd.nist.gov)

- **17794 PHP win32std extension arbitrary code execution Vulnerability**

Buffer overflow in php_win32std.dll in the win32std extension for PHP 5.2.0 and earlier allows context-dependent attackers to execute arbitrary code via a long string in the filename argument to the win_browse_file function.

The vulnerability has been confirmed in version 5.x up to 5.2.0 included.

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

References:

* MILW0RM: 4293
http://www.milw0rm.com/exploits/4293
* BID: 25414
http://www.securityfocus.com/bid/25414
* XF: php-phpwin32sti-bo(36118)
http://xforce.iss.net/xforce/xfdb/36118

CVE Reference:

CVE-2007-4441 (cve.mitre.org, nvd.nist.gov)

- **17795 PHP php_ntuser component arbitrary code execution and denial of service Vulnerabilities**

Multiple buffer overflows in the php_ntuser component for PHP 5.2.3 allow context-dependent attackers to cause a denial of service or execute arbitrary code via long arguments to the ntuser_getuserlist, ntuser_getuserinfo, ntuser_getusergroups, or ntuser_getdomaincontroller functions.

The vulnerability has been confirmed in version 5.x up to 5.2.3 included.

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

References:

* MILW0RM: 4304
http://www.milw0rm.com/exploits/4304

CVE Reference:

CVE-2007-4507 (cve.mitre.org, nvd.nist.gov)

- **17796 PHP iisfunc extension arbitrary code execution Vulnerability**

Multiple buffer overflows in php_iisfunc.dll in the iisfunc extension for PHP 5.2.0 and earlier allow context-dependent attackers to execute arbitrary code, probably during Unicode conversion, as demonstrated by a long string in the first argument to the iis_getservicestate function, related to the ServiceId argument to the fnStartService, fnGetServiceState, fnStopService, and possibly other functions.

The vulnerability has been confirmed in version 5.x up to 5.2.0 included.

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

References:

* MILW0RM: 4318
http://www.milw0rm.com/exploits/4318
* BID: 25452
http://www.securityfocus.com/bid/25452
* XF: php-phpiisfunc-bo(36262)
http://xforce.iss.net/xforce/xfdb/36262

CVE Reference:

CVE-2007-4586 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

Apple Safari on Windows Code Execution Vulnerability

"Execution of arbitrary code"

A vulnerability has been reported in Apple Safari in combination with Microsoft Windows, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a combination of errors related to the default download location in Safari and the Windows desktop handling of executables.

Successful exploitation allows execution of arbitrary code when a user visits a malicious web site.

The vulnerability is reported in Safari running on Windows XP or Vista.

References:
http://www.microsoft.com/technet/security/advisory/953818.mspx

VMware Products Multiple Vulnerabilities

"Execute arbitrary code"

Some vulnerabilities have been reported in multiple VMware products, which can be exploited by malicious, local users to bypass certain security restrictions.

1) A boundary error exists in the implementation of the Host Guest File System (HGFS). This can be exploited to cause a heap-based buffer overflow in the context of the "vmx" process on the host system.

Successful exploitation requires that shared folders are enabled and at least one folder is

shared on the host (not by default).

2) An unspecified error in the Virtual Machine Communication Interface (VMCI) implementation can be exploited to execute arbitrary code in the context of the "vmx" process on the host system.

Successful exploitation requires that VMCI is enabled and that the VMware host is running on Windows.

References:
http://www.vmware.com/security/advisories/VMSA-2008-0008.html

HP StorageWorks Storage Mirroring Software Unspecified Code Execution

"Execution of arbitrary code"

A vulnerability has been reported in HP StorageWorks Storage Mirroring Software, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified error. No further information is currently available.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in version 4.5 Service Pack 1.

References:
https://www12.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01362558

Apache Tomcat Host Manager "name" Cross-Site Scripting

"Cross-site scripting attacks"

A vulnerability has been reported in Tomcat, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed via the "name" parameter to host-manager/html/add is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a logged in user's browser session in context of an affected site.

The vulnerability is reported in version 5.5.9 through 5.5.26 and 6.0.0 to 6.0.16.

References:
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html

Asterisk "pedantic" SIP Processing Denial of Service

"Denial of Service"

A vulnerability has been reported in Asterisk, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL-pointer dereference error in the

"ast_uri_decode()" function. This can be exploited to crash the application via a SIP message lacking a "From" field.

Successful exploitation requires that "pedantic" processing is enabled.

The vulnerability is reported in the following products:
* Asterisk Open Source 1.0.x (all versions)
* Asterisk Open Source 1.2.x (all versions prior to 1.2.29)
* Asterisk Business Edition A.x.x (all versions)
* Asterisk Business Edition B.x.x (all versions prior to B.2.5.3)

References:
http://downloads.digium.com/pub/security/AST-2008-008.html

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