

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

[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.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

New worm targets industrial control systems. US doing cyberattack simulation. Charges in Zeus trojan crimes. Guide to Windows 7 security.

This week the team behind SecureScout submitted and got approved 4 patches to the well known security tool Nmap. These patches relate to memory allocation issues and inconsistencies in the Nmap OS fingerprint database file. Nmap is massively used in the security industry especially by pen-testers, vulnerability assessment products, and hackers. Nmap was featured in the movie "Matrix Reloaded".

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

• Stuxnet should serve as wake-up call, say experts

Experts say that the Stuxnet worm should serve as a wake-up call that cyberwarfare against critical infrastructure systems is a reality.

"Up until now, the discussions have been scenario-based," Dave Marcus, director of security research at McAfee Avert Labs, told SCMagazineUS.com on Tuesday. "Here is an actual, real-world example. It's not conceptual anymore."

Stuxnet is a sophisticated worm that was designed to target industrial control systems software manufactured by Siemens, Andy Hayter, anti-malcode manager at security solutions tester ICSA Labs, wrote in a blog post late last week. SC Magazine

Full Story :

http://www.scmagazineus.com/stuxnet-should-serve-as-wake-up-call-say-experts/article/179858/?utm_source=feedb

• U.S. testing defenses with simulated cyberattack

The U.S. government has launched a full-scale simulated cyberattack to gauge how the country might fare in the real thing.

Sponsored by the Department of Homeland Security, Cyber Storm III kicked off yesterday for a three-day series of simulated events designed to exploit holes in the nation's cybersecurity system.

Specifically, the exercise will "inject" more than 1,500 different types of threats to examine the ability of the people involved to prepare for cyberattacks, make the correct decisions to respond to them, and share sensitive information with the right parties. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20017840-83.html?part=rss&subj=news&tag=2547-1_3-0-20

• Dozens charged in use of Zeus Trojan to steal \$3 million

The FBI and the U.S. Attorney's office in southern New York announced charges today against 37 people accused of being part of an international crime ring that stole \$3 million from bank accounts by infecting computers with the Zeus Trojan and other malware.

Between federal and state charges, more than 60 people total are being charged in the operation, officials said.

Ten people were arrested today by federal and New York law enforcement officers and another 10 were previously arrested in the U.S. as part of a coordinated takedown, authorities said. Seventeen people are still being sought in the U.S. and abroad, officials said. The defendants named in the documents, unsealed by the court today, were all listed as being from Eastern Europe and face federal charges. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20018177-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• The InfoWorld expert guide to Windows 7 security

InfoWorld - Windows 7 has been warmly received and swiftly adopted by businesses, with the result that many IT admins are now struggling with the platform's new security features. In addition to changes to User Account Control, BitLocker, and other features inherited from Windows Vista, Windows 7 introduces a slew of new security capabilities that businesses will want to take advantage of.

Windows 7 improves on Vista with a friendlier UAC mechanism, the ability to encrypt removable media as well as hard drive volumes, broader support for strong cryptographic ciphers, hassle-free secure remote access, and sophisticated protection against Trojan malware in the form of AppLocker, to name just a few.

[Get the full scoop on getting more value from your log files in the InfoWorld "Windows 7 Security Deep Dive" PDF special report. | Better manage your company's information security with our Security Central newsletter.] Computerworld

Full Story :

http://www.computerworld.com/s/article/9188878/The_InfoWorld_expert_guide_to_Windows_7_security?source=rss

New Vulnerabilities Tested in SecureScout

• 18942 WordPad Word 97 Text Converter Memory Corruption Vulnerability (MS10-067/2259922) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft WordPad processes memory when parsing a specially crafted Word 97 document. The vulnerability could allow remote code execution if a user opens a specially crafted Word file that includes a malformed structure.

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

References:

* MS: MS10-067

<http://www.microsoft.com/technet/security/Bulletin/MS10-067.msp>

* BID: 43122

<http://www.securityfocus.com/bid/43122>

* VUPEN: VUPEN/ADV-2010-2388

<http://www.vupen.com/english/advisories/2010/2388>

* SECTRACK: 1024442

<http://securitytracker.com/alerts/2010/Sep/1024442.html>

CVE Reference:

CVE-2010-2563 (cve.mitre.org, nvd.nist.gov)

• 18943 MPEG Layer-3 Audio Decoder Buffer Overflow Vulnerability (MS10-052/2115168) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft DirectShow MP3 filter handles supported format files. This vulnerability could allow code execution if a user opened a specially crafted audio file. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS10-052

<http://www.microsoft.com/technet/security/Bulletin/MS10-052.msp>

* CERT: TA10-222A

<http://www.us-cert.gov/cas/techalerts/TA10-222A.html>

* OVAL: oval:org.mitre.oval:def:11585

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11585>

* BID: 42298

<http://www.securityfocus.com/bid/42298>

* SECTRACK: 1024302

<http://securitytracker.com/alerts/2010/Aug/1024302.html>

* VUPEN: VUPEN/ADV-2010-2049

<http://www.vupen.com/english/advisories/2010/2049>

CVE Reference:

CVE-2010-1882 (cve.mitre.org, nvd.nist.gov)

• 18944 Cinepak Codec Decompression Vulnerability (MS10-055/982665) (Remote File Checking)

A remote code execution vulnerability exists in the way the Cinepak codec handles supported format files. This vulnerability could allow code execution if a user opened a specially crafted media file. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* SECTRACK: 1024304

<http://securitytracker.com/alerts/2010/Aug/1024304.html>

* VUPEN: VUPEN/ADV-2010-2052

<http://www.vupen.com/english/advisories/2010/2052>

* MS: MS10-055

<http://www.microsoft.com/technet/security/Bulletin/MS10-055.msp>

* CERT: TA10-222A

<http://www.us-cert.gov/cas/techalerts/TA10-222A.html>

* OVAL: oval:org.mitre.oval:def:11773

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11773>

CVE Reference:

CVE-2010-2553 (cve.mitre.org, nvd.nist.gov)

• 18945 Microsoft Silverlight Memory Corruption Vulnerability (MS10-060/2265906) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Silverlight handles pointers. The vulnerability could allow remote code execution if a user visits a specially crafted Web site that contains Silverlight content.

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

References:

- * SECTRACK: 1024306
<http://securitytracker.com/alerts/2010/Aug/1024306.html>
- * VUPEN: VUPEN/ADV-2010-2057
<http://www.vupen.com/english/advisories/2010/2057>
- * MS: MS10-055
<http://www.microsoft.com/technet/security/Bulletin/MS10-055.mspx>
- * CERT: TA10-222A
<http://www.us-cert.gov/cas/techalerts/TA10-222A.html>
- * OVAL: oval:org.mitre.oval:def:11773
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11773>
- * BID: 42138
<http://www.securityfocus.com/bid/42138>

CVE Reference:

CVE-2010-0019 (cve.mitre.org, nvd.nist.gov)

• 18946 Microsoft Silverlight and Microsoft .NET Framework CLR Virtual Method Delegate Vulnerability (MS10-060/2265906) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft .NET Framework that can allow a specially crafted Microsoft .NET application or a specially crafted Silverlight application to access memory, leading to arbitrary unmanaged code execution.

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

References:

- * SECTRACK: 1024306
<http://securitytracker.com/alerts/2010/Aug/1024306.html>
- * VUPEN: VUPEN/ADV-2010-2057
<http://www.vupen.com/english/advisories/2010/2057>
- * BID: 42295
<http://www.securityfocus.com/bid/42295>
- * MS: MS10-060
<http://www.microsoft.com/technet/security/Bulletin/MS10-060.mspx>
- * CERT: TA10-222A
<http://www.us-cert.gov/cas/techalerts/TA10-222A.html>
- * OVAL: oval:org.mitre.oval:def:12033
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12033>

CVE Reference:

CVE-2010-1898 (cve.mitre.org, nvd.nist.gov)

• 18947 Movie Maker Memory Corruption Vulnerability (MS10-050/981997) (Remote File Checking)

A remote code execution vulnerability exists in the way that Windows Movie Maker handles specially crafted project files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * SECTRACK: 1024309
<http://securitytracker.com/alerts/2010/Aug/1024309.html>
- * VUPEN: VUPEN/ADV-2010-2047
<http://www.vupen.com/english/advisories/2010/2047>
- * BID: 42268
<http://www.securityfocus.com/bid/42268>
- * MS: MS10-050
<http://www.microsoft.com/technet/security/Bulletin/MS10-050.mspx>
- * CERT: TA10-222A
<http://www.us-cert.gov/cas/techalerts/TA10-222A.html>
- * OVAL: oval:org.mitre.oval:def:12011
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12011>

CVE Reference:

CVE-2010-2564 (cve.mitre.org, nvd.nist.gov)

• **18948 Wireshark SigComp Universal Decompressor Virtual Machine buffer overflow Vulnerability (CVE-2010-2995) (Remote File Checking)**

The SigComp Universal Decompressor Virtual Machine (UDVM) in Wireshark 0.10.8 through 1.0.14 and 1.2.0 through 1.2.9 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to sigcomp-udvm.c and an off-by-one error, which triggers a buffer overflow, different vulnerabilities than CVE-2010-2287.

The vulnerability is reported in versions 0.10.8 up to and including 1.0.14, 1.2.0 up to and including 1.2.9.

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

References:

* CONFIRM:

<http://www.wireshark.org/docs/relnotes/wireshark-1.2.10.html>

* CONFIRM:

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4867

* OVAL: oval:org.mitre.oval:def:12049

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12049>

* CONFIRM: wnpa-sec-2010-07

<http://www.wireshark.org/security/wnpa-sec-2010-07.html>

CVE Reference:

CVE-2010-2995 (cve.mitre.org, nvd.nist.gov)

• **18949 Wireshark ASN.1 BER dissector stack memory exhaustion Vulnerability (Remote File Checking)**

Stack-based buffer overflow in the ASN.1 BER dissector in Wireshark 0.10.13 through 1.0.14 and 1.2.0 through 1.2.9 has unknown impact and remote attack vectors. NOTE: this issue exists because of a CVE-2010-2284 regression.

The vulnerability is reported in versions 0.10.13 up to and including 1.0.14, 1.2.0 up to and including 1.2.9.

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

References:

* CONFIRM:

<http://www.wireshark.org/docs/relnotes/wireshark-1.2.10.html>

* OVAL: oval:org.mitre.oval:def:12047

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12047>

* CONFIRM: wnpa-sec-2010-07

<http://www.wireshark.org/security/wnpa-sec-2010-07.html>

CVE Reference:

CVE-2010-2994 (cve.mitre.org, nvd.nist.gov)

• **18950 Wireshark GSM A RR dissector could crash Vulnerability (Remote File Checking)**

packet-gsm_a_rr.c in the GSM A RR dissector in Wireshark 1.2.2 through 1.2.9 allows remote attackers to cause a denial of service (crash) via unknown vectors that trigger a NULL pointer dereference.

The vulnerability is reported in versions 1.2.2 up to and including 1.2.9.

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

References:

* CONFIRM: wnpa-sec-2010-08

<http://www.wireshark.org/security/wnpa-sec-2010-08.html>

* CONFIRM:

<http://www.wireshark.org/docs/relnotes/wireshark-1.2.10.html>

* CONFIRM:

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4897

* OVAL: oval:org.mitre.oval:def:11651

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11651>

CVE Reference:

CVE-2010-2992 (cve.mitre.org, nvd.nist.gov)

• 18951 Wireshark The IPMI dissector could go into an infinite loop Vulnerability (Remote File Checking)

The IPMI dissector in Wireshark 1.2.0 through 1.2.9 allows remote attackers to cause a denial of service (infinite loop) via unknown vectors.

The vulnerability is reported in versions 1.2.0 up to and including 1.2.9.

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

References:

* CONFIRM: wnpa-sec-2010-08

<http://www.wireshark.org/security/wnpa-sec-2010-08.html>

* CONFIRM:

<http://www.wireshark.org/docs/relnotes/wireshark-1.2.10.html>

* OVAL: [oval:org.mitre.oval:def:12031](http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12031)

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12031>

CVE Reference:

CVE-2010-2993 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-2950 PHP CVSS 2.0 Score = 6.8

Format string vulnerability in stream.c in the phar extension in PHP 5.3.x through 5.3.3 allows context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted phar:// URI that is not properly handled by the phar_stream_flush function, leading to errors in the php_stream_wrapper_log_error function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2094.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=598537

CONFIRM: <http://svn.php.net/viewvc?view=revision&revision=302565>

CONFIRM: <http://security-tracker.debian.org/tracker/CVE-2010-2950>

MISC:

http://php-security.org/2010/05/14/mops-2010-024-php-phar_stream_flush-format-string-vulnerability/index.html

SUSE: <http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

CVE Reference: [CVE-2010-2950](http://cve.mitre.org)

• CVE-2010-3087 Novell CVSS 2.0 Score = 6.8

LibTIFF before 3.9.2-5.2.1 in SUSE openSUSE 11.3 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted TIFF image.

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

References:

CONFIRM: https://bugzilla.novell.com/show_bug.cgi?id=624215

CONFIRM: <http://support.novell.com/security/cve/CVE-2010-3087.html>

SUSE: <http://lists.opensuse.org/opensuse-security-announce/2010-09/msg00006.html>

CVE Reference: [CVE-2010-3087](http://cve.mitre.org)

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