

2010 Issue #30

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 privacy bill under critics. Dell reacts to malware in motherboards. The price of being popular? Microsoft announces new initiative around vulnerability reporting.

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

• Tech firms warn privacy bill will harm economy

Captions, from left: Rep. Rush (D), witnesses being sworn in, Rep. Whitfield (R), Mike Zaneis from Interactive Advertising Bureau

(Credit: U.S. House of Representatives) A new privacy bill introduced in the U.S. Congress this week would have serious unintended consequences and could even harm the nation's economy unless its Democratic sponsor rewrites it, Internet industry representatives warned Thursday.

The proposal, introduced by Rep. Bobby Rush of Illinois, slaps fines of up to \$5 million on businesses and even some individuals unless they abide by a complex set of new regulations to be administrated by the Federal Trade Commission. Cnet Security

Full Story :

http://news.cnet.com/8301-31921_3-20011435-281.html?part=rss&subj=news&tag=2547-1_3-0-20

• Dell revamps hardware testing in wake of malware issue

IDG News Service - A sequence of errors led to Dell's delivery of motherboards with malware and the company is in the process of overhauling its testing process to resolve issues before dispatching hardware to customers, it said on Thursday.

Dell on Wednesday said that some replacement motherboards for PowerEdge servers may have contained the W32.Spybot worm in flash storage. The malware issue affected a limited number of replacement motherboards in four servers, the PowerEdge R310, PowerEdge R410, PowerEdge R510 and PowerEdge T410 models, the company said.

"There was a sequence of human errors that led to the issue, That being said, we have identified and implemented 16 additional process steps to make sure this doesn't happen again," said Dell spokesman Jim Hahn. Computerworld

Full Story :

http://www.computerworld.com/s/article/9179556/Dell_revamps_hardware_testing_in_wake_of_malware_issue?source=hp

• Secunia: Apple software has the most holes

A new report from security software provider Secunia shows that despite considerable security investments, the software industry at large is unable to produce software with substantially fewer vulnerabilities.

The latest data shows that Apple has surpassed Oracle and even Microsoft with accounting for the most software vulnerabilities, though the No. 1 ranking is related only to the number of vulnerabilities--not to how risky they are or how fast they get patched.

Makers of software with the most vulnerabilities Cnet Security

Full Story :

http://news.cnet.com/8301-13846_3-20011403-62.html?part=rss&subj=news&tag=2547-1_3-0-20

• Microsoft announces "coordinated" plan for bug reporting

Calling the term "responsible disclosure" too subjective, Microsoft on Thursday announced a new initiative around vulnerability reporting that seeks to align efforts between researchers and vendors.

Labeling the practice "coordinated vulnerability disclosure," Microsoft is hoping to silence the ongoing debate over how software, hardware and service flaws are reported to vendors by researchers - and how both parties should appropriately respond. The issue came to head recently when a Google researcher, in a post on Full Disclosure, released details about a Windows vulnerability after he was unable to negotiate a timeline for a fix with Microsoft. sc Magazine

Full Story :

http://www.scmagazineus.com/microsoft-announces-coordinated-plan-for-bug-reporting/article/175170/?utm_source=hp

New Vulnerabilities Tested in SecureScout

• 14589 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2207) (Remote File Checking)

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.

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

References:

* SECTRACK: 1024159

<http://securitytracker.com/alerts/2010/Jun/1024159.html>

* VUPEN: VUPEN/ADV-2010-1636

<http://www.vupen.com/english/advisories/2010/1636>

* BID: 41239

<http://www.securityfocus.com/bid/41239>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

CVE Reference:

CVE-2010-2207 (cve.mitre.org, nvd.nist.gov)

• **14590 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2208) (Rmote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, dereference a heap object after this object's deletion, which allows attackers to execute arbitrary code via unspecified vectors.

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

References:

- * SECTRACK: 1024159
<http://securitytracker.com/alerts/2010/Jun/1024159.html>
- * VUPEN: VUPEN/ADV-2010-1636
<http://www.vupen.com/english/advisories/2010/1636>
- * BID: 41244
<http://www.securityfocus.com/bid/41244>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

CVE Reference:

CVE-2010-2208 (cve.mitre.org, nvd.nist.gov)

• **14591 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2209) (Rmote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.

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

References:

- * SECTRACK: 1024159
<http://securitytracker.com/alerts/2010/Jun/1024159.html>
- * VUPEN: VUPEN/ADV-2010-1636
<http://www.vupen.com/english/advisories/2010/1636>
- * BID: 41240
<http://www.securityfocus.com/bid/41240>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

CVE Reference:

CVE-2010-2209 (cve.mitre.org, nvd.nist.gov)

• **14592 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2210) (Rmote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2211, and CVE-2010-2212.

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

References:

- * SECTRACK: 1024159
<http://securitytracker.com/alerts/2010/Jun/1024159.html>
- * VUPEN: VUPEN/ADV-2010-1636
<http://www.vupen.com/english/advisories/2010/1636>
- * BID: 41242
<http://www.securityfocus.com/bid/41242>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

CVE Reference:

CVE-2010-2210 (cve.mitre.org, nvd.nist.gov)

• **14593 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2211) (Rmote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, and CVE-2010-2212.

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

References:

- * SECTRACK: 1024159
<http://securitytracker.com/alerts/2010/Jun/1024159.html>
- * VUPEN: VUPEN/ADV-2010-1636
<http://www.vupen.com/english/advisories/2010/1636>
- * BID: 41243
<http://www.securityfocus.com/bid/41243>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

CVE Reference:

CVE-2010-2211 (cve.mitre.org, nvd.nist.gov)

• 18205 Mailslot Heap Overflow Vulnerability (MS06-035/917159) (Network Check)

There is a remote code execution vulnerability in the Server driver that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:

- * BUGTRAQ: 20060711 TSRT-06-02: Microsoft SRV.SYS Mailslot Ring0 Memory Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/439773/100/0/threaded>
- * MISC:
<http://www.tippingpoint.com/security/advisories/TSRT-06-02.html>
- * MS: MS06-035
<http://www.microsoft.com/technet/security/bulletin/ms06-035.msp>
- * CERT: TA06-192A
<http://www.us-cert.gov/cas/techalerts/TA06-192A.html>
- * CERT-VN: VU#189140
<http://www.kb.cert.org/vuls/id/189140>
- * BID: 18863
<http://www.securityfocus.com/bid/18863>
- * VUPEN: ADV-2006-2753
<http://www.vupen.com/english/advisories/2006/2753>
- * OSVDB: 27154
<http://www.osvdb.org/27154>
- * OVAL: oval:org.mitre.oval:def:600
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:600>
- * SECUNIA: 21007
<http://secunia.com/advisories/21007>
- * SREASON: 1212
<http://securityreason.com/securityalert/1212>
- * XF: win-mailslot-bo(26818)
<http://xforce.iss.net/xforce/xfdb/26818>

CVE Reference:

CVE-2006-1314 (cve.mitre.org, nvd.nist.gov)

• 18855 SMB Information Disclosure Vulnerability (MS06-035/917159) (Network Check)

There is an information disclosure vulnerability in the Server service that could allow an attacker to view fragments of memory used to store SMB traffic during transport.

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

References:

- * BUGTRAQ: 20060711 SMB Information Disclosure Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/439881/100/0/threaded>
- * MS: MS06-035
<http://www.microsoft.com/technet/security/bulletin/ms06-035.msp>
- * CERT-VN: VU#333636

<http://www.kb.cert.org/vuls/id/333636>

* BID: 18891

<http://www.securityfocus.com/bid/18891>

* VUPEN: ADV-2006-2753

<http://www.vupen.com/english/advisories/2006/2753>

* OSVDB: 27155

<http://www.osvdb.org/27155>

* OVAL: oval:org.mitre.oval:def:3

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3>

* SECTRACK: 1016467

<http://securitytracker.com/id?1016467>

* SECUNIA: 21007

<http://secunia.com/advisories/21007>

* XF: win-smb-information-disclosure(26820)

<http://xforce.iss.net/xforce/xfdb/26820>

CVE Reference:

CVE-2006-1315 (cve.mitre.org, nvd.nist.gov)

• 18856 SMB Buffer Overflow Remote Code Execution Vulnerability (MS09-001/958687) (Network Check)

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could take complete control of the system. Most attempts to exploit this vulnerability would result in a system denial of service condition, however remote code execution is theoretically possible.

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

References:

* BUGTRAQ: 20090113 ZDI-09-001: Microsoft SMB NT Trans Request Parsing Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/500012/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-09-001/>

* MS: MS09-001

<http://www.microsoft.com/technet/security/bulletin/ms09-001.msp>

* CERT: TA09-013A

<http://www.us-cert.gov/cas/techalerts/TA09-013A.html>

* BID: 33121

<http://www.securityfocus.com/bid/33121>

* OVAL: oval:org.mitre.oval:def:5863

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5863>

* VUPEN: ADV-2009-0116

<http://www.frsirt.com/english/advisories/2009/0116>

* SECTRACK: 1021560

<http://www.securitytracker.com/id?1021560>

CVE Reference:

CVE-2008-4834 (cve.mitre.org, nvd.nist.gov)

• 18857 SMB Validation Remote Code Execution Vulnerability (MS09-001/958687) (Network Check)

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could cause the attacker to take complete control of the system. Most attempts to exploit this vulnerability would result in a system denial of service condition, however remote code execution is theoretically possible.

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

References:

* BUGTRAQ: 20090113 ZDI-09-002: Microsoft SMB NT Trans2 Request Parsing Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/500013/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-09-002/>

* MS: MS09-001

<http://www.microsoft.com/technet/security/bulletin/ms09-001.msp>

* CERT: TA09-013A

<http://www.us-cert.gov/cas/techalerts/TA09-013A.html>

* BID: 33122

<http://www.securityfocus.com/bid/33122>

* OVAL: oval:org.mitre.oval:def:5248

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5248>

* VUPEN: ADV-2009-0116

<http://www.frsirt.com/english/advisories/2009/0116>

* SECTRACK: 1021560

<http://www.securitytracker.com/id?1021560>

CVE Reference:

CVE-2008-4835 (cve.mitre.org, nvd.nist.gov)

• 18858 SMB Validation Denial of Service Vulnerability (MS09-001/958687) (Network Check)

A denial of service vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and restart.

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

References:

* BUGTRAQ: 20080914 Microsoft Windows WRITE_ANDX SMB command handling Kernel DoS

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

* MILW0RM: 6463

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

* MISC:

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

* MISC:

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

* MS: MS09-001

<http://www.microsoft.com/technet/security/bulletin/ms09-001.msp>

* CERT: TA09-013A

<http://www.us-cert.gov/cas/techalerts/TA09-013A.html>

* BID: 31179

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

* OVAL: oval:org.mitre.oval:def:5262

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5262>

* OVAL: oval:org.mitre.oval:def:6044

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6044>

* VUPEN: ADV-2008-2583

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

* SECTRACK: 1020887

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

* SECUNIA: 31883

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

* XF: win-writeandx-dos(45146)

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

CVE Reference:

CVE-2008-4114 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-2568 Microsoft CVSS 2.0 Score = 9.3

Windows Shell in Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users or remote attackers to execute arbitrary code via a crafted (1) .LNK or (2) .PIF shortcut file, which is not properly handled during icon display in Windows Explorer, as demonstrated in the wild in July 2010, and originally reported for malware that leverages CVE-2010-2772 in Siemens WinCC SCADA systems.

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

References:

CERT-VN: <http://www.kb.cert.org/vuls/id/940193>

BID: <http://www.securityfocus.com/bid/41732>

CONFIRM: <http://www.microsoft.com/technet/security/advisory/2286198.msp>

MISC: http://www.f-secure.com/weblog/archives/new_rootkit_en.pdf

MISC: <http://www.f-secure.com/weblog/archives/00001986.html>

SECTRAK: <http://securitytracker.com/id?1024216>

SECUNIA: <http://secunia.com/advisories/40647>

MISC: <http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/>

MISC: <http://isc.sans.edu/diary.html?storyid=9190>

MISC: <http://isc.sans.edu/diary.html?storyid=9181>

CVE Reference: [CVE-2010-2568](#)

• **CVE-2010-1973 HP CVSS 2.0 Score = 6.8**

Unspecified vulnerability in the Auditing subsystem in HP OpenVMS 8.3, 8.2, 7.3-2, and earlier on the ALPHA platform, and 8.3-1H1, 8.3, 8.2-1, and earlier on the Itanium platform, allows local users to gain privileges or obtain sensitive information via unknown vectors. Per: <http://marc.info/?l=bugtraq&m=127905660900687&w=2> 'impacted versions are listed. HP OpenVMS ALPHA v 8.3, v 8.2, v 7.3-2 and earlier HP OpenVMS Itanium v 8.3-1H1, v 8.3, v 8.2-1 and earlier'

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

References:

HP: <http://marc.info/?l=bugtraq&m=127905660900687&w=2>

HP: <http://marc.info/?l=bugtraq&m=127905660900687&w=2>

SECTRAK: <http://securitytracker.com/id?1024190>

CVE Reference: [CVE-2010-1973](#)

• **CVE-2010-1972 HP CVSS 2.0 Score = 5.0**

The default configuration of HP Client Automation (HPCA) Enterprise Infrastructure (aka Radia) allows remote attackers to read log files, and consequently cause a denial of service or have unspecified other impact, via web requests.

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

References:

SECTRAK: <http://securitytracker.com/id?1024191>

SECUNIA: <http://secunia.com/advisories/40592>

HP: <http://marc.info/?l=bugtraq&m=127905601332098&w=2>

HP: <http://marc.info/?l=bugtraq&m=127905601332098&w=2>

CVE Reference: [CVE-2010-1972](#)

• **CVE-2010-1969 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in HP Virtual Connect Enterprise Manager for Windows before 6.1 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.

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

References:

HP:

http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02283465&admit=109447626+1279054975923+2835

HP:

http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02283465&admit=109447626+1279054975923+2835

VUPEN: <http://www.vupen.com/english/advisories/2010/1797>

SECTRAK: <http://www.securitytracker.com/id?1024181>

SECUNIA: <http://secunia.com/advisories/40552>

CVE Reference: [CVE-2010-1969](#)

• **CVE-2010-2771 IBM CVSS 2.0 Score = 10.0**

solid.exe in IBM solidDB before 6.5 FP2 allows remote attackers to execute arbitrary code via a long username field in the first handshake packet.

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

References:

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-10-125/>

BID: <http://www.securityfocus.com/bid/41653>

SECTRAK: <http://securitytracker.com/id?1024203>

MISC:

<http://publib.boulder.ibm.com/infocenter/soliddb/v6r5/index.jsp?topic=/com.ibm.swg.im.soliddb.common.doc/doc/detailed.l>

CVE Reference: [CVE-2010-2771](#)

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