

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

Spammers and scammers use World cup. Global fraud ring busted. Senate consider increased power to president to fight cyber crime. iPad site hole disclosed by hackers.

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

• World Cup lottery spam, targeted malware discovered

Cybercriminals are keeping their foot on the gas as the month-long World Cup soccer tournament in South Africa continues.

A number of scams are underway this week to spread malware and trick users into handing over sensitive information, security researchers warned.

One phishing campaign discovered this week appears to be a new take on the "Nigerian 419" scams. SC Magazine

Full Story :

http://www.scmagazineus.com/world-cup-lottery-spam-targeted-malware-discovered/article/172701/?utm_source=feed

• Police bust massive global credit card fraud ring

Police in 12 countries have arrested 178 individuals linked to an international credit card fraud ring. According to a statement from the Spanish Interior Ministry, the arrests were the result of a two-year investigation that included 84 raids carried out in France, Italy, Germany, Ireland, Romania, Australia, Sweden, Greece, Finland, Hungary and the United States.

The gang used stolen bank card numbers to create counterfeit cards and make ATM withdrawals and retail purchases, officials said. Police raids yielded more than 5,000 counterfeit cards and 120,000 stolen card numbers. Additionally, authorities found 11 laboratories where members of the group produced the fraudulent cards.

Police also believe the gang engaged in other criminal activities, including robbery with force, fraud, extortion, sexual exploitation and money laundering, earning \$24.5 million from its illegal activities. SC Magazine

Full Story :

http://www.scmagazineus.com/police-bust-massive-global-credit-card-fraud-ring/article/172617/?utm_source=feedbu

• Senate bill would expand government cybersecurity role

A Senate Committee is set to consider a bill that would grant the president emergency power over critical infrastructure networks, in addition to create cybersecurity offices within the White House and U.S. Department of Homeland Security (DHS).

The Protecting Cyberspace as a National Asset Act of 2010, introduced last Thursday by Sens. Joe Lieberman, I-Conn.; Susan Collins, R-Maine and Tom Carper, D-Del, is intended to strengthen and coordinate the security of federal civilian and critical infrastructure networks.

Critics, however, worry the bill may give too much power to government in controlling systems and networks interlinked with the private sector. SC Magazine

Full Story :

http://www.scmagazineus.com/senate-bill-would-expand-government-cybersecurity-role/article/172542/?utm_source

• Hackers were right to disclose AT&T-iPad site hole

commentary If you are an iPad 3G user, it's possible that your e-mail address is in the hands of malicious hackers who could send you e-mails with malware targeted to infect your device. There's also the possibility--albeit much slimmer--that someone could use the serial number for your device to get more information on you and even track your whereabouts.

That's because of a hole in AT&T's customer Web site for iPad 3G users that became public last week. (You can read more details about it here.)

AT&T issued an apology to its affected iPad 3G customers this weekend, but the company mostly used the e-mail to blame the hackers who discovered the problem instead of accepting responsibility for its own security oversight. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20007701-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 18828 Excel Record Parsing Memory Corruption Vulnerability (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

* VUPEN: VUPEN/ADV-2010-1395

<http://www.vupen.com/english/advisories/2010/1395>

* SECTRAK: 1024076

<http://securitytracker.com/alerts/2010/Jun/1024076.html>

* BID: 40518

<http://www.securityfocus.com/bid/40518>

* BUGTRAQ: 20100608 ZDI-10-104: Microsoft Office Excel SxView Record Parsing Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/511729/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-104>

* MS: MS10-038

<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-0821 (cve.mitre.org, nvd.nist.gov)

• 18829 Excel Object Stack Overflow Vulnerability (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

* VUPEN: VUPEN/ADV-2010-1395

<http://www.vupen.com/english/advisories/2010/1395>

* SECTRAK: 1024076

<http://securitytracker.com/alerts/2010/Jun/1024076.html>

* MS: MS10-038

<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

* BID: 40520

<http://www.securityfocus.com/bid/40520>

* OSVDB: 65236

<http://osvdb.org/65236>

CVE Reference:

CVE-2010-0822 (cve.mitre.org, nvd.nist.gov)

• 18830 Excel Memory Corruption Vulnerability (CVE-2010-0823) (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

* VUPEN: VUPEN/ADV-2010-1395

<http://www.vupen.com/english/advisories/2010/1395>

* SECTRAK: 1024076

<http://securitytracker.com/alerts/2010/Jun/1024076.html>

* MS: MS10-038

<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

* OSVDB: 65233

<http://osvdb.org/65233>

* BID: 40521

<http://www.securityfocus.com/bid/40521>

CVE Reference:

CVE-2010-0823 (cve.mitre.org, nvd.nist.gov)

• 18831 Excel Record Memory Corruption Vulnerability (CVE-2010-0824) (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

- * VUPEN: VUPEN/ADV-2010-1395
<http://www.vupen.com/english/advisories/2010/1395>
- * SECTRAK: 1024076
<http://securitytracker.com/alerts/2010/Jun/1024076.html>
- * MS: MS10-038
<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * BID: 40522
<http://www.securityfocus.com/bid/40522>

CVE Reference:

CVE-2010-0824 (cve.mitre.org, nvd.nist.gov)

• 18832 Excel Record Memory Corruption Vulnerability (CVE-2010-1245) (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

- * VUPEN: VUPEN/ADV-2010-1395
<http://www.vupen.com/english/advisories/2010/1395>
- * SECTRAK: 1024076
<http://securitytracker.com/alerts/2010/Jun/1024076.html>
- * MS: MS10-038
<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * BID: 40523
<http://www.securityfocus.com/bid/40523>

CVE Reference:

CVE-2010-1245 (cve.mitre.org, nvd.nist.gov)

• 18833 Excel RTD Memory Corruption Vulnerability (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

- * VUPEN: VUPEN/ADV-2010-1395
<http://www.vupen.com/english/advisories/2010/1395>
- * SECTRAK: 1024076
<http://securitytracker.com/alerts/2010/Jun/1024076.html>
- * BID: 40524
<http://www.securityfocus.com/bid/40524>
- * MS: MS10-038
<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

CVE Reference:

CVE-2010-1246 (cve.mitre.org, nvd.nist.gov)

• 18834 Excel Memory Corruption Vulnerability (CVE-2010-1247) (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

- * VUPEN: VUPEN/ADV-2010-1395
<http://www.vupen.com/english/advisories/2010/1395>
- * SECTRAK: 1024076
<http://securitytracker.com/alerts/2010/Jun/1024076.html>
- * BID: 40525
<http://www.securityfocus.com/bid/40525>
- * MS: MS10-038
<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * OSVDB: 65237
<http://osvdb.org/65237>

CVE Reference:

CVE-2010-1247 (cve.mitre.org, nvd.nist.gov)

• 18835 Excel HFPicture Memory Corruption Vulnerability (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

- * VUPEN: VUPEN/ADV-2010-1395
<http://www.vupen.com/english/advisories/2010/1395>
- * SECTRAK: 1024076
<http://securitytracker.com/alerts/2010/Jun/1024076.html>
- * MS: MS10-038
<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * BID: 40526
<http://www.securityfocus.com/bid/40526>
- * OSVDB: 65235
<http://osvdb.org/65235>

CVE Reference:

CVE-2010-1248 (cve.mitre.org, nvd.nist.gov)

• 18836 Excel Memory Corruption Vulnerability (CVE-2010-1249) (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

- * VUPEN: VUPEN/ADV-2010-1395
<http://www.vupen.com/english/advisories/2010/1395>
- * SECTRAK: 1024076
<http://securitytracker.com/alerts/2010/Jun/1024076.html>
- * MS: MS10-038
<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * BID: 40527
<http://www.securityfocus.com/bid/40527>
- * OSVDB: 65232
<http://osvdb.org/65232>

CVE Reference:

CVE-2010-1249 (cve.mitre.org, nvd.nist.gov)

• **18837 Excel EDG Memory Corruption Vulnerability (MS10-038/2027452) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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:

- * VUPEN: VUPEN/ADV-2010-1395
<http://www.vupen.com/english/advisories/2010/1395>
- * SECTRAK: 1024076
<http://securitytracker.com/alerts/2010/Jun/1024076.html>
- * MS: MS10-038
<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * BID: 40528
<http://www.securityfocus.com/bid/40528>

CVE Reference:

CVE-2010-1250 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2010-1885 Microsoft CVSS 2.0 Score = 9.3**

The MPC::HexToNum function in helpctr.exe in Microsoft Windows Help and Support Center in Windows XP and Windows Server 2003 does not properly handle malformed escape sequences, which allows remote attackers to bypass the trusted documents whitelist (fromHCP option) and execute arbitrary commands via a crafted hcp:// URL.

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

References:

- CERT-VN: <http://www.kb.cert.org/vuls/id/578319>
- XF: <http://xforce.iss.net/xforce/xfdb/59267>
- VUPEN: <http://www.vupen.com/english/advisories/2010/1417>
- SECTRAK: <http://www.securitytracker.com/id?1024084>
- BID: <http://www.securityfocus.com/bid/40725>
- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/511783/100/0/threaded>
- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/511774/100/0/threaded>
- CONFIRM: <http://www.microsoft.com/technet/security/advisory/2219475.msp>
- SECUNIA: <http://secunia.com/advisories/40076>
- CONFIRM: <http://blogs.technet.com/b/srd/archive/2010/06/10/help-and-support-center-vulnerability-full-disclosure-posting.aspx>
- MISC: <http://blogs.technet.com/b/msrc/archive/2010/06/10/windows-help-vulnerability-disclosure.aspx>
- FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2010-06/0197.html>

CVE Reference: [CVE-2010-1885](#)

• **CVE-2010-2265 Microsoft CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in the GetServerName function in sysinfo/commonFunc.js in Microsoft Windows Help and Support Center for Windows XP and Windows Server 2003 allows remote attackers to inject arbitrary web script or HTML via the svr parameter to sysinfo/sysinfo/main.htm. NOTE: this can be leveraged with

CVE-2010-1885 to execute arbitrary commands without user interaction.

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

References:

CERT-VN: <http://www.kb.cert.org/vuls/id/578319>

XF: <http://xforce.iss.net/xforce/xfdb/59267>

VUPEN: <http://www.vupen.com/english/advisories/2010/1417>

BID: <http://www.securityfocus.com/bid/40721>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/511774/100/0/threaded>

MISC: <http://www.microsoft.com/technet/security/advisory/2219475.msp>

SECUNIA: <http://secunia.com/advisories/40076>

MISC:
<http://blogs.technet.com/b/srd/archive/2010/06/10/help-and-support-center-vulnerability-full-disclosure-posting.aspx>

MISC: <http://blogs.technet.com/b/msrc/archive/2010/06/10/windows-help-vulnerability-disclosure.aspx>

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2010-06/0197.html>

CVE Reference: [CVE-2010-2265](#)

• **CVE-2010-2305 Symantec CVSS 2.0 Score = 9.3**

Buffer overflow in an ActiveX control in SSHelper.dll for Symantec Sygate Personal Firewall 5.6 build 2808 allows remote attackers to execute arbitrary code via a long third argument to the SetRegString method.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/59408>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/13834>

MISC:
<http://www.corelan.be:8800/index.php/forum/security-advisories/10-050-sygate-personal-firewall-5-6-build-2808-activex/>

CVE Reference: [CVE-2010-2305](#)

• **CVE-2010-2279 IBM CVSS 2.0 Score = 7.6**

The Top Updates implementation in the Homepage component in IBM Lotus Connections 2.5.x before 2.5.0.2, when "forced SSL" is enabled, uses http for links, which has unspecified impact and remote attack vectors.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21431472>

VUPEN: <http://www.vupen.com/english/advisories/2010/1281>

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1LO48325>

SECUNIA: <http://secunia.com/advisories/40007>

CVE Reference: [CVE-2010-2279](#)

• **CVE-2009-3793 Adobe CVSS 2.0 Score = 9.3**

Unspecified vulnerability in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory consumption) or possibly execute arbitrary code via unknown vectors.

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

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb10-14.html>

BID: <http://www.securityfocus.com/bid/40759>

SECTrack: <http://securitytracker.com/id?1024086>

SECTrack: <http://securitytracker.com/id?1024085>

CVE Reference: [CVE-2009-3793](#)

• **CVE-2010-2160 Adobe CVSS 2.0 Score = 9.3**

Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.

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

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb10-14.html>

BID: <http://www.securityfocus.com/bid/40759>

SECTrack: <http://securitytracker.com/id?1024086>

SECTrack: <http://securitytracker.com/id?1024085>

CVE Reference: [CVE-2010-2160](#)

• **CVE-2010-2161 Adobe CVSS 2.0 Score = 9.3**

Array index error in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified "types of Adobe Flash code."

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

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb10-14.html>

BID: <http://www.securityfocus.com/bid/40759>

SECTrack: <http://securitytracker.com/id?1024086>

SECTrack: <http://securitytracker.com/id?1024085>

CVE Reference: [CVE-2010-2161](#)

• **CVE-2010-2162 Adobe CVSS 2.0 Score = 9.3**

Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (heap memory corruption) or possibly execute arbitrary code via unspecified vectors.

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

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb10-14.html>

BID: <http://www.securityfocus.com/bid/40759>

SECTrack: <http://securitytracker.com/id?1024086>

SECTrack: <http://securitytracker.com/id?1024085>

CVE Reference: [CVE-2010-2162](#)

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