

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://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

Targeted attacks take over spam. New Windows 7 bug found. U.S. Chamber of Commerce hacked for extended time period. 55 charged with cyber fraud.

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

• Spam drop, but targeted attack rise, is key 2011 takeaway

As cybercriminals more heavily rely on targeted attacks, the amount of spam this year fell to the lowest levels since 2007, according to Cisco. The volume of unsolicited email dropped dramatically, from 379 billion messages daily in August 2010 to 124 billion last month, according to Cisco's "2011 Annual Security Report," released Wednesday. One reason for the change - mass mailing campaigns are simply not as lucrative as targeted malware efforts.

While the latter requires just one or a few people to be duped to churn out a large payday for the perpetrator, mass spam campaigns typically require a much higher response rate to be profitable.

The amount of spam emanating from the United States fell sharply in 2011. Compared to last year, when the U.S. was the world's largest spam-sender, the country ranked ninth in total spam volume worldwide during 2011. SC Magazine

Full Story :

http://www.scmagazineus.com/spam-drop-but-targeted-attack-rise-is-key-2011-takeaway/article/220252/?utm_source

• **Researcher finds Microsoft Windows 7 security bug**

A researcher has taken to Twitter to warn of a Windows vulnerability that can be exploited through Apple's Safari browser.

The hybrid flaw, which vulnerability management firm Secunia confirmed in an advisory, is caused by a weakness in the driver file of Win32, which is a core interface used by Windows to communicate with the programs that run on it.

Secunia confirmed the validity of the vulnerability, which it deemed "highly critical," on a fully patched Windows 7 Professional 64-bit machine. Earlier versions of the operating system also may be affected. SC Magazine

Full Story :

http://www.scmagazineus.com/researcher-finds-microsoft-windows-7-security-bug/article/220253/?utm_source=feed

• **U.S. Chamber of Commerce targeted in data heist**

Hackers believed to be from China may have had reign over the U.S. Chamber of Commerce's network for more than a year before a devastating breach was detected, according to a Wednesday report.

According to a story in Wednesday's editions of The Wall Street Journal, a known hacker group operating out of China infiltrated the network of the U.S. Chamber, the world's largest lobbying group representing some three million American businesses, from at least November 2009 to May 2010, but possibly longer.

Citing people familiar with the matter, the newspaper said the intruders came and went "as they pleased" thanks to "backdoors" and tactics used to cover their tracks. SC Magazine

Full Story :

http://www.scmagazineus.com/us-chamber-of-commerce-targeted-in-data-heist/article/220439/?utm_source=feed

• **NYC authorities charge 55 in cyber fraud, ID theft ring**

The Manhattan district attorney's office on Friday announced the indictments of 55 individuals charged with stealing millions of dollars from multiple financial institutions as part of a massive cyber fraud scheme. The defendants, many of whom reside in Brooklyn, N.Y., are accused of stealing more than \$2 million from Chase, TD Bank, Citibank, Discover and American Express, Manhattan District Attorney Cyrus Vance announced Friday. As part of their scheme, the crime ring also stole the identities of at least 200 individuals and organizations. The charges include conspiracy to commit grand larceny, grand larceny, criminal possession of stolen property, identity theft and criminal possession of a forged instrument.

Between May 2010 and September 2011, the perpetrators allegedly relied on rogue insiders at banks and other businesses to steal the personal information, including Social Security numbers and financial account information, belonging to unsuspecting customers, prosecutors said. SC Magazine

Full Story :

http://www.scmagazineus.com/nyc-authorities-charge-55-in-cyber-fraud-id-theft-ring/article/220013/?utm_source=feed

• **U.S. Chamber of Commerce targeted in data heist**

Hackers believed to be from China may have had reign over the U.S. Chamber of Commerce's network for more than a year before a devastating breach was detected, according to a Wednesday report.

According to a story in Wednesday's editions of The Wall Street Journal, a known hacker group operating out of China infiltrated the network of the U.S. Chamber, the world's largest lobbying group representing some 300,000 American businesses, from at least November 2009 to May 2010, but possibly longer.

Citing people familiar with the matter, the newspaper said the intruders came and went "as they pleased" thanks to "backdoors" and tactics used to cover their tracks. SC Magazine

Full Story :

http://www.scmagazineus.com/us-chamber-of-commerce-targeted-in-data-heist/article/220439/?utm_source=feed

New Vulnerabilities Tested in SecureScout

• **19696 Microsoft Windows OLE Property Vulnerability**

Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 do not properly handle OLE objects in memory, which allows remote attackers to execute arbitrary code via a crafted object in a file, aka "OLE Property Vulnerability."

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

References:

- * MS: MS11-093
<http://technet.microsoft.com/security/bulletin/MS11-093>
- * BID: 50977
<http://www.securityfocus.com/bid/50977>
- * SECUNIA: 47207
<http://secunia.com/advisories/47207/>

CVE Reference:

CVE-2011-3400 (cve.mitre.org, nvd.nist.gov)

• 19697 Microsoft Office Word Use-after-free vulnerability

Use-after-free vulnerability in Microsoft Office 2007 SP2 and SP3 and Office 2010 SP1 allows remote attackers to execute arbitrary code via a crafted Word document, aka "Word Use After Free Vulnerability".

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

References:

- * MS: MS11-089
<http://technet.microsoft.com/security/bulletin/MS11-089>
- * URL: CVE-2011-1983
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1983>
- * SECUNIA: CVE-2011-1983
http://secunia.com/advisories/cve_reference/CVE-2011-1983/

CVE Reference:

CVE-2011-1983 (cve.mitre.org, nvd.nist.gov)

• 19698 Microsoft Windows CSRSS Local Privilege Elevation Vulnerability

Csrsvr.dll in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 SP1 does not properly check permissions for sending inter-process device-event messages from low-integrity processes to high-integrity processes, which allows local users to gain privileges via a crafted application, aka "CSRSS Local Privilege Elevation Vulnerability."

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

References:

- * MS: MS11-097
<http://technet.microsoft.com/security/bulletin/MS11-097>
- * SECUNIA: CVE-2011-3408
http://secunia.com/advisories/cve_reference/CVE-2011-3408/
- * URL: win-ms11kb2620712-update.htm
http://www.iss.net/security_center/reference/vuln/win-ms11kb2620712-update.htm

CVE Reference:

CVE-2011-3408 (cve.mitre.org, nvd.nist.gov)

• 19699 Internet Explorer XSS Filter Information Disclosure Vulnerability

The XSS Filter in Microsoft Internet Explorer 8 allows remote attackers to read content from a different (1) domain or (2) zone via a "trial and error" attack, aka "XSS Filter Information Disclosure Vulnerability."

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

References:

- * MS: MS11-099
<http://technet.microsoft.com/security/bulletin/MS11-099>
- * SECUNIA: CVE-2011-1992
http://secunia.com/advisories/cve_reference/CVE-2011-1992/
- * URL: CVE-2011-1992
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1992>
- * BID: 50959
<http://www.securityfocus.com/bid/50959>

CVE Reference:

CVE-2011-1992 (cve.mitre.org, nvd.nist.gov)

• 19700 Internet Explorer Insecure Library Loading Vulnerability

Untrusted search path vulnerability in Microsoft Internet Explorer 9 on Windows Server 2008 R2 and R2 SP1 and Windows 7 SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains an HTML file, aka "Internet Explorer Insecure Library Loading Vulnerability."

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

References:

- * MS: MS11-099
<http://technet.microsoft.com/security/bulletin/MS11-099>
- * SECUNIA: cve_reference/CVE-2011-2019/
http://secunia.com/advisories/cve_reference/CVE-2011-2019/
- * SECTRAK: tracker/CVE-2011-2019
<http://security-tracker.debian.org/tracker/CVE-2011-2019>
- * BID: 50975/info
<http://www.securityfocus.com/bid/50975/info>

CVE Reference:

CVE-2011-2019 (cve.mitre.org, nvd.nist.gov)

• 19701 Internet Explorer Content-Disposition Information Disclosure Vulnerability

Microsoft Internet Explorer 6 through 9 does not properly use the Content-Disposition HTTP header to control rendering of the HTTP response body, which allows remote attackers to read content from a different (1) domain or (2) zone via a crafted web site, aka "Content-Disposition Information Disclosure Vulnerability."

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

References:

- * MS: MS11-099
<http://technet.microsoft.com/security/bulletin/MS11-099>

CVE Reference:

CVE-2011-3404 (cve.mitre.org, nvd.nist.gov)

• 19702 Windows Media Player DVR-MS Memory Corruption Vulnerability

ENCDEC.DLL in Windows Media Player and Media Center in Microsoft Windows XP SP2 and SP3, Windows Vista SP2, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted .dvr-ms file, aka "Windows Media Player DVR-MS Memory Corruption Vulnerability."

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

References:

- * SECUNIA: CVE-2011-3401
http://secunia.com/advisories/cve_reference/CVE-2011-3401/
- * MS: MS11-092
<http://technet.microsoft.com/security/bulletin/MS11-092>
- * URL:
<https://www.infosecisland.com/alertsview/18720-CVE-2011-3401-windows7-windowsvista-windowsxp.html>
- * BID:
<http://www.securityfocus.com/bid/50957>

CVE Reference:

CVE-2011-3401 (cve.mitre.org, nvd.nist.gov)

• 19704 Microsoft Windows Kernel Exception Handler Vulnerability

The kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, and Windows 7 SP1 does not properly initialize objects, which allows local users to gain privileges via a crafted application, aka "Windows Kernel Exception Handler Vulnerability."

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

References:

- * MS: MS11-098
<http://technet.microsoft.com/security/bulletin/MS11-098>

* NETVIGILANCE-UNKNOWN: bid/50969
<http://www.securityfocus.com/bid/50969>
* SECUNIA: cve_reference/CVE-2011-2018/
http://secunia.com/advisories/cve_reference/CVE-2011-2018/

CVE Reference:

CVE-2011-2018 (cve.mitre.org, nvd.nist.gov)

• 19705 Microsoft Office PowerPoint PowerPoint Insecure Library Loading Vulnerability

Untrusted search path vulnerability in Microsoft PowerPoint 2007 SP2 and 2010 allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka "PowerPoint Insecure Library Loading Vulnerability."

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

References:

* MS: MS11-094
<http://technet.microsoft.com/security/bulletin/MS11-094>
* SECUNIA: cve_reference/CVE-2011-3396/
http://secunia.com/advisories/cve_reference/CVE-2011-3396/
* SECTRAK: tracker/CVE-2011-3396
<http://security-tracker.debian.org/tracker/CVE-2011-3396>

CVE Reference:

CVE-2011-3396 (cve.mitre.org, nvd.nist.gov)

• 19706 Microsoft Windows Win32k TrueType font handling remote code execution vulnerability

Unspecified vulnerability in the Win32k TrueType font parsing engine in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via crafted font data in a Word document, as exploited in the wild in November 2011 by Duqu.

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

References:

* BID: bid/50462
<http://www.securityfocus.com/bid/50462>
* MISC:
<http://blogs.mcafee.com/mcafee-labs/the-day-of-the-golden-jackal-%E2%80%93-further-foes-of-the-stuxnet-files>
* MISC:
http://www.securelist.com/en/blog/208193197/The_Mystery_of_Duqu_Part_Two
* MISC:
http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit
* MISC:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the
* MISC:
http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-291-01E.pdf
* CONFIRM:
<http://blogs.technet.com/b/msrc/archive/2011/11/03/microsoft-releases-security-advisory-2639658.aspx>
* CONFIRM:
<http://technet.microsoft.com/security/advisory/2639658>
* MS: MS11-087
<http://technet.microsoft.com/security/bulletin/MS11-087>

CVE Reference:

CVE-2011-3402 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-3660 Mozilla CVSS 2.0 Score = 10.0

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 8.0, Thunderbird 5.0 through 8.0, and SeaMonkey before 2.6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors that trigger a compartment mismatch associated with the nsDOMMessageEvent::GetData function, and unknown other vectors.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=706249
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=701637
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=701248
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=700512
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=697255
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=696579
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=694200
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=693144
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=693143
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=691873
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=691746
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=690376
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=689892
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=688974
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=688364
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=686107
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=685321
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=685186
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=682252
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=680687
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=679986
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=679494
CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=562442
CONFIRM: <http://www.mozilla.org/security/announce/2011/mfsa2011-53.html>

CVE Reference: [CVE-2011-3660](#)

• **CVE-2011-3658 Mozilla CVSS 2.0 Score = 7.5**

The SVG implementation in Mozilla Firefox 8.0, Thunderbird 8.0, and SeaMonkey 2.5 does not properly interact with DOMAttrModified event handlers, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via vectors involving removal of SVG elements.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=708186
CONFIRM: <http://www.mozilla.org/security/announce/2011/mfsa2011-55.html>

CVE Reference: [CVE-2011-3658](#)

• **CVE-2011-3665 Mozilla CVSS 2.0 Score = 7.5**

Mozilla Firefox 4.x through 8.0, Thunderbird 5.0 through 8.0, and SeaMonkey before 2.6 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an Ogg VIDEO element that is not properly handled after scaling.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=701259

CONFIRM: <http://www.mozilla.org/security/announce/2011/mfsa2011-58.html>

CVE Reference: [CVE-2011-3665](https://cve.mitre.org/cve/2011/3665)

• **CVE-2011-3661 Mozilla CVSS 2.0 Score = 7.5**

YARR, as used in Mozilla Firefox 4.x through 8.0, Thunderbird 5.0 through 8.0, and SeaMonkey before 2.6, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted JavaScript.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=691299

CONFIRM: <http://www.mozilla.org/security/announce/2011/mfsa2011-54.html>

CVE Reference: [CVE-2011-3661](https://cve.mitre.org/cve/2011/3661)

• **CVE-2011-3666 Mozilla CVSS 2.0 Score = 6.8**

Mozilla Firefox before 3.6.25 and Thunderbird before 3.1.17 on Mac OS X do not consider .jar files to be executable files, which allows user-assisted remote attackers to bypass intended access restrictions via a crafted file. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-2372 on Mac OS X.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=704622

CONFIRM: <http://www.mozilla.org/security/announce/2011/mfsa2011-59.html>

CVE Reference: [CVE-2011-3666](https://cve.mitre.org/cve/2011/3666)

• **CVE-2011-3664 Mozilla CVSS 2.0 Score = 6.8**

Mozilla Firefox before 9.0, Thunderbird before 9.0, and SeaMonkey before 2.6 on Mac OS X do not properly handle certain DOM frame deletions by plugins, which allows remote attackers to cause a denial of service (incorrect pointer dereference and application crash) or possibly have unspecified other impact via a crafted web site. Per: <http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=649079

CONFIRM: <http://www.mozilla.org/security/announce/2011/mfsa2011-57.html>

CVE Reference: [CVE-2011-3664](https://cve.mitre.org/cve/2011/3664)

• **CVE-2011-3663 Mozilla CVSS 2.0 Score = 4.3**

Mozilla Firefox 4.x through 8.0, Thunderbird 5.0 through 8.0, and SeaMonkey before 2.6 allow remote attackers to capture keystrokes entered on a web page by using SVG animation accessKey events within that web page.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=704482

CONFIRM: <http://www.mozilla.org/security/announce/2011/mfsa2011-56.html>

CVE Reference: [CVE-2011-3663](https://cve.mitre.org/cve/2011/3663)

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