

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

netVigilance wishes a happy and prosperous New Year to all.

Weirdest news from 2011. Oops... Fix for asp.net vulnerability. Vulnerability in wireless router setup.

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

• Book of Lists: 2011's strongest trends, weirdest news

Top 3 weirdest news items Taste of one's own medicine: A hacker in October who received a scam email had the last laugh when he took control of the phishing page and turned it into a public service announcement around phishing awareness.

Happy ending: Ivan Kaspersky, who was kidnapped for a ransom of \$4.3 million, was rescued following a police operation. He is the son of IT security mogul and Kaspersky Lab founder Eugene, one of the wealthiest businessmen in Russia.

Mean streets: The YouTube channel for Sesame Street was briefly hijacked by hackers who swapped out educational videos with X-rated pornography. Not long after, Microsoft's YouTube channel was also compromised, but not to display erotic video. SC Magazine

Full Story :

http://www.scmagazine.com/book-of-lists-2011s-strongest-trends-weirdest-news/article/221189/?utm_source=feedbu

• **Email from The New York Times meant for 300, sent to 8M**

An email asking people to reconsider their cancellation of home delivery from The New York Times accidentally was sent to some eight million people on Wednesday, but was intended to reach only a few hundred.

Twitter lit up on Wednesday afternoon EST over reports from users who received the message but were confused, considering they either didn't cancel their existing subscription or didn't have a plan to begin with. Even a parody account was set up within minutes of the first report.

Robert Christie, a Times spokesman, initially tweeted that the emails appeared to be spam. But minutes later, that was recanted in a tweet from Amy Chozick, a corporate media reporter for the paper. SC Magazine

Full Story :

http://www.scmagazine.com/email-from-the-new-york-times-meant-for-300-sent-to-8m/article/221021/?utm_source=fe

• **Microsoft delivers rare out-of-band patch for ASP.NET issue**

Microsoft's engineers on Thursday gave IT administrators a late Christmas present: a fix for an unpatched and publicly known vulnerability affecting the software giant's ASP.NET web application framework.

One day after disclosing the flaw, which affects ASP.NET versions 1.1 and later on all supported versions of the .NET Framework, Microsoft released an emergency patch, which also addresses three other bugs, all of which were privately reported.

"An attacker who successfully exploited this vulnerability could take any action in the context of an existing account on the ASP.NET site, including executing arbitrary commands," the bulletin from Microsoft said. SC Magazine

Full Story :

http://www.scmagazine.com/microsoft-delivers-rare-out-of-band-patch-for-aspnet-issue/article/221187/?utm_source=fe

• **Vulnerability allows brute force hacking of wireless routers**

A computing standard that enables users to easily stand up an encrypted wireless network suffers from a design weakness that could enable attackers to gain router access, according to US-CERT.

The vulnerability exists in the WiFi Protected Setup (WPS) and could allow an adversary to brute force the standard's authentication method, drastically reducing the number of attempts necessary to retrieve the router's PIN password. With this in hand, the adversary can change the access point's configuration and launch a denial-of-service attack.

"When the PIN authentication fails, the access point will send [a message] back to the client," according to a US-CERT advisory. "The...messages are sent in a way that an attacker is able to determine if the first half of the PIN is correct. Also, the last digit of the PIN is known because it is a checksum for the PIN." SC Magazine

Full Story :

http://www.scmagazine.com/vulnerability-allows-brute-force-hacking-of-wireless-routers/article/221016/?utm_source=fe

New Vulnerabilities Tested in SecureScout

• **19687 Mozilla Firefox multiple unspecified vulnerabilities in the browser engine (CVE-2011-2997)**

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-36.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=655098

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=660453

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=662215

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=665360

* DEBIAN: DSA-2312

<http://www.debian.org/security/2011/dsa-2312>

* DEBIAN: DSA-2313
<http://www.debian.org/security/2011/dsa-2313>
* DEBIAN: DSA-2317
<http://www.debian.org/security/2011/dsa-2317>
* MANDRIVA: MDVSA-2011:139
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:139>
* MANDRIVA: MDVSA-2011:140
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:140>
* MANDRIVA: MDVSA-2011:141
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:141>
* MANDRIVA: MDVSA-2011:142
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:142>
* REDHAT: RHSA-2011:1341
<http://www.redhat.com/support/errata/RHSA-2011-1341.html>
* SUSE: openSUSE-SU-2011:1076
<http://lists.opensuse.org/opensuse-updates/2011-10/msg00002.html>
* SECUNIA: 46315
<http://secunia.com/advisories/46315>

CVE Reference:

CVE-2011-2997 (cve.mitre.org, nvd.nist.gov)

• 19688 Mozilla Firefox handling "location" vulnerability (CVE-2011-2999)

Mozilla Firefox before 3.6.23 and 4.x through 5 do not properly handle "location" as the name of a frame, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, a different vulnerability than CVE-2010-0170.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-38.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=665548
* DEBIAN: DSA-2312
<http://www.debian.org/security/2011/dsa-2312>
* DEBIAN: DSA-2313
<http://www.debian.org/security/2011/dsa-2313>
* DEBIAN: DSA-2317
<http://www.debian.org/security/2011/dsa-2317>
* MANDRIVA: MDVSA-2011:139
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:139>
* MANDRIVA: MDVSA-2011:140
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:140>
* MANDRIVA: MDVSA-2011:141
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:141>
* REDHAT: RHSA-2011:1341
<http://www.redhat.com/support/errata/RHSA-2011-1341.html>
* SUSE: openSUSE-SU-2011:1076
<http://lists.opensuse.org/opensuse-updates/2011-10/msg00002.html>
* SECUNIA: 46315
<http://secunia.com/advisories/46315>

CVE Reference:

CVE-2011-2999 (cve.mitre.org, nvd.nist.gov)

• 19689 Mozilla Firefox handling HTTP responses vulnerability (CVE-2011-3000)

Mozilla Firefox before 3.6.23 and 4.x through 6 do not properly handle HTTP responses that contain multiple Location, Content-Length, or Content-Disposition headers, which makes it easier for remote attackers to conduct HTTP response splitting attacks via crafted header values.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-39.html>
* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=655389

* DEBIAN: DSA-2312

<http://www.debian.org/security/2011/dsa-2312>

* DEBIAN: DSA-2313

<http://www.debian.org/security/2011/dsa-2313>

* DEBIAN: DSA-2317

<http://www.debian.org/security/2011/dsa-2317>

* MANDRIVA: MDVSA-2011:139

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:139>

* MANDRIVA: MDVSA-2011:140

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:140>

* MANDRIVA: MDVSA-2011:141

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:141>

* MANDRIVA: MDVSA-2011:142

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:142>

* REDHAT: RHSA-2011:1341

<http://www.redhat.com/support/errata/RHSA-2011-1341.html>

* SUSE: openSUSE-SU-2011:1076

<http://lists.opensuse.org/opensuse-updates/2011-10/msg00002.html>

* SECUNIA: 46315

<http://secunia.com/advisories/46315>

CVE Reference:

CVE-2011-3000 (cve.mitre.org, nvd.nist.gov)

• 19690 Mozilla Firefox returning value of a GrowAtomTable function call vulnerability (CVE-2011-3002)

Almost Native Graphics Layer Engine (ANGLE), as used in Mozilla Firefox before 7.0 does not validate the return value of a GrowAtomTable function call, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger a memory-allocation error and a resulting buffer overflow.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-41.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=680840

* MANDRIVA: MDVSA-2011:141

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:141>

CVE Reference:

CVE-2011-3002 (cve.mitre.org, nvd.nist.gov)

• 19695 Microsoft Office PowerPoint OfficeArt Shape RCE Vulnerability (CVE-2011-3413)

Microsoft PowerPoint 2007 SP2 and PowerPoint Viewer 2007 SP2 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via an invalid OfficeArt record in a PowerPoint document, aka "OfficeArt Shape RCE Vulnerability."

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

References:

* MS: MS11-094

<http://technet.microsoft.com/security/bulletin/MS11-094>

* BID: 50964

<http://www.securityfocus.com/bid/50964>

* SECUNIA: CVE-2011-3413

http://secunia.com/advisories/cve_reference/CVE-2011-3413/

CVE Reference:

CVE-2011-3413 (cve.mitre.org, nvd.nist.gov)

• 19707 Microsoft Office Excel Record Memory Corruption Vulnerability (CVE-2011-3403)

Microsoft Excel 2003 SP3 do not properly handle objects in memory, which allows remote attackers to execute arbitrary code via a crafted Excel spreadsheet, aka "Record Memory Corruption Vulnerability."

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

References:

- * MS: MS11-096
<http://technet.microsoft.com/security/bulletin/MS11-096>
- * SECUNIA: cve_reference/CVE-2011-3403/
http://secunia.com/advisories/cve_reference/CVE-2011-3403/
- * URL: bid=50954
http://www.symantec.com/security_response/vulnerability.jsp?bid=50954

CVE Reference:

CVE-2011-3403 (cve.mitre.org, nvd.nist.gov)

• 19708 Microsoft Publisher Function Pointer Overwrite Vulnerability (CVE-2011-1508)

Microsoft Publisher 2003 SP3, and 2007 SP2 and SP3, does not properly manage memory allocations for function pointers, which allows user-assisted remote attackers to execute arbitrary code via a crafted Publisher file, aka "Publisher Function Pointer Overwrite Vulnerability."

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

References:

- * MS: MS11-091
<http://technet.microsoft.com/security/bulletin/MS11-091>
- * BID:
<http://www.securityfocus.com/bid/50090>
- * SECUNIA:
http://secunia.com/advisories/cve_reference/CVE-2011-1508/

CVE Reference:

CVE-2011-1508 (cve.mitre.org, nvd.nist.gov)

• 19709 Microsoft Publisher Out-of-bounds Array Index Vulnerability (CVE-2011-3410)

Array index error in Microsoft Publisher 2003 SP3, and 2007 SP2 and SP3, allows remote attackers to execute arbitrary code via a crafted Publisher file that leverages incorrect handling of values in memory, aka "Publisher Out-of-bounds Array Index Vulnerability."

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

References:

- * MS: MS11-091
<http://technet.microsoft.com/security/bulletin/MS11-091>
- * URL: 2607702
[http://about-threats.trendmicro.com/Vulnerability.aspx?language=us&name=\(MS11-091\)](http://about-threats.trendmicro.com/Vulnerability.aspx?language=us&name=(MS11-091)) Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2607702)
- * SECUNIA: CVE-2011-3410
http://secunia.com/advisories/cve_reference/CVE-2011-3410/
- * BID: 50943
<http://www.securityfocus.com/bid/50943>

CVE Reference:

CVE-2011-3410 (cve.mitre.org, nvd.nist.gov)

• 19710 Microsoft Publisher Invalid Pointer Vulnerability (CVE-2011-3411)

Microsoft Publisher 2003 SP3 allows remote attackers to execute arbitrary code via a crafted Publisher file that leverages incorrect handling of values in memory, aka "Publisher Invalid Pointer Vulnerability."

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

References:

- * MS: MS11-091
<http://technet.microsoft.com/security/bulletin/MS11-091>
- * SECUNIA: CVE-2011-3411
http://secunia.com/advisories/cve_reference/CVE-2011-3411/
- * URL: alert=CVE-2011-3411
<http://www.security-database.com/detail.php?alert=CVE-2011-3411>
- * URL: CVE-2011-3411.html
<http://leic.lumension.com/vulnerabilities/2011/CVE-2011-3411.html>
- * BID: 50949

<http://www.securityfocus.com/bid/50949>

CVE Reference:

CVE-2011-3411 (cve.mitre.org, nvd.nist.gov)

• **19711 Microsoft Publisher Memory Corruption Vulnerability (CVE-2011-3412)**

Microsoft Publisher 2003 SP3, and 2007 SP2 and SP3, allows remote attackers to execute arbitrary code via a crafted Publisher file that leverages incorrect memory handling, aka "Publisher Memory Corruption Vulnerability."

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

References:

* MS: MS11-091

<http://technet.microsoft.com/security/bulletin/MS11-091>

* URL: bid=50955

http://www.symantec.com/security_response/vulnerability.jsp?bid=50955

* URL: ba-p/121842

<http://forums.juniper.net/t5/Networking-Security-Now/December-2011-Microsoft-Patch-Tuesday-Summary/ba-p/121842>

* BID: 50955

<http://www.securityfocus.com/bid/50955>

CVE Reference:

CVE-2011-3412 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2007-6750 Apache CVSS 2.0 Score = 5.0**

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.

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

References:

MISC: <http://hackers.org/slowloris/>

BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2007-01/0229.html>

CVE Reference: [CVE-2007-6750](http://cve.mitre.org/cve/2007/6750)

• **CVE-2011-4165 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP Database Archiving Software 6.31 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1263.

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

References:

HP: <http://marc.info/?l=bugtraq&m=132517846332173&w=2>

HP: <http://marc.info/?l=bugtraq&m=132517846332173&w=2>

CVE Reference: [CVE-2011-4165](http://cve.mitre.org/cve/2011/4165)

• **CVE-2011-4164 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP Database Archiving Software 6.31 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1214.

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

References:

HP: <http://marc.info/?l=bugtraq&m=132517846332173&w=2>

HP: <http://marc.info/?l=bugtraq&m=132517846332173&w=2>

CVE Reference: [CVE-2011-4164](http://cve.mitre.org/cve/2011/4164)

• **CVE-2011-4163 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP Database Archiving Software 6.31 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1213.

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

References:

HP: <http://marc.info/?l=bugtraq&m=132517846332173&w=2>

HP: <http://marc.info/?l=bugtraq&m=132517846332173&w=2>

CVE Reference: [CVE-2011-4163](#)

• **CVE-2011-4169 HP CVSS 2.0 Score = 7.5**

Unspecified vulnerability in HP Managed Printing Administration before 2.6.4 allows remote attackers to obtain sensitive information, modify data, or cause a denial of service via unknown vectors.

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

References:

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03128469>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03128469>

CVE Reference: [CVE-2011-4169](#)

• **CVE-2011-4167 HP CVSS 2.0 Score = 7.5**

Stack-based buffer overflow in MPAUploader.dll in HP Managed Printing Administration before 2.6.4 allows remote attackers to execute arbitrary code via a long filename parameter in an uploadfile action to Default.asp.

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

References:

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-353/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03128469>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03128469>

CVE Reference: [CVE-2011-4167](#)

• **CVE-2011-4166 HP CVSS 2.0 Score = 7.5**

Directory traversal vulnerability in the MPAUploader.Uploader.1.UploadFiles method in HP Managed Printing Administration before 2.6.4 allows remote attackers to create arbitrary files via crafted form data.

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

References:

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-352/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03128469>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03128469>

CVE Reference: [CVE-2011-4166](#)

• **CVE-2011-4168 HP CVSS 2.0 Score = 7.5**

Directory traversal vulnerability in hmpa/jobDelivery/Default.asp in HP Managed Printing Administration before 2.6.4 allows remote attackers to create arbitrary files via crafted form data.

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

References:

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-354/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03128469>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03128469>

CVE Reference: [CVE-2011-4168](#)

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