

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

SSL certificate industry standard on the way. Most claims against Heartland dismissed. Yahoo wins over spammers. Fewer critical Microsoft bugs.

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

• Industry group creates guidelines for issuing SSL certs

A consortium of certificate authorities (CAs) and software vendors has released the first industry standard for the issuance and management of SSL certificates. The standard follows a series of embarrassing attacks this year against CAs, or companies that sell the digital SSL or TLS certificates, which are used by websites to validate their identity to visitors. The document, "Baseline Requirement for the Issuance and Management of Publicly Trusted Certificates," released by the CA/Browser Forum, is described as the first international standard for the operation of CAs that issue digital certs.

"SSL/TLS certificates are a critical part of the internet's security infrastructure," Tim Moses, chairman of the CA/Browser Forum, said in a news release. "The new baseline requirements will improve the reliability and accountability of SSL/TLS issuance." SC Magazine

Full Story :

http://www.scmagazineus.com/industry-group-creates-guidelines-for-issuing-ssl-certs/article/219595/?utm_source=

• Court tosses claims against Heartland Payment over breach

A U.S. District judge has thrown out most claims brought forth by banks against Heartland Payment Systems following a 2008 breach of the payment card processor's systems that exposed an estimated 130 million credit and debit card numbers to organized criminals. Dozens of separate lawsuits, on behalf of consumers and banks, were filed against Princeton, N.J.-based Heartland, which disclosed in January 2009 that its systems were breached. In June 2009, the U.S. Judicial Panel on Multidistrict Litigation decided the civil complaints against Heartland would be consolidated and heard in Texas, where Heartland's IT personnel are based. The cases were divided into two tracks, one for consumer plaintiffs and another for financial institution plaintiffs.

After more than two years of litigation, District Judge Lee Rosenthal earlier this month dismissed nine of the 10 causes of action brought forth as part of a class-action lawsuit by nine banks. The banks had claimed they incurred significant expenses when they replaced payment cards and reimbursed fraudulent transactions as a result of the breach. SC Magazine

Full Story :

http://www.scmagazineus.com/court-tosses-claims-against-heartland-payment-over-breach/article/219129/?utm_source=

• Yahoo wins \$610M spam judgment

Digital media company Yahoo ended a three-year legal battle against a team of spammers, winning a default judgment of \$610 million on Dec. 5.

The defendants - a group of Thai and Nigerian individuals and corporations - had been charged with running a lottery fraud scam for several years, in which hoax emails purportedly from Yahoo were sent informing recipients they had won large sums of money. When someone responded, they were sent back a message informing them they needed to pay a fee prior to collecting their winnings.

The emails intended to establish credibility by counterfeiting the Yahoo name and trademark, and thus mislead recipients into believing that the messages were sent or authorized by the web giant, the memorandum order stated. SC Magazine

Full Story :

http://www.scmagazineus.com/yahoo-wins-610m-spam-judgment/article/218793/?utm_source=feedburner&utm_medium=

• "Critical" Microsoft security bugs at lowest level since 2005

Microsoft patched fewer "critical" security vulnerabilities this year than it did in any other year since 2005, the company said Tuesday. The Redmond, Wash.-based computing giant issued 99 security bulletins during 2011, with 13 released Tuesday during its final patch batch of the year, Mike Reavey, director of the Microsoft Security Response Center, said in a blog post Tuesday. Thirty-two percent of all bulletins issued this year were tagged with Microsoft's highest severity rating of critical. During the last six months of 2011, the percentage was lower, with 20 percent of all patches listed as critical.

Not since 2004, the year Microsoft first began issuing monthly security patches, has the percentage of critical bulletins in a given year been so low. Moreover, in terms of absolute numbers, critical vulnerabilities, or the most severe type of flaw - whose exploitation could result in the spread of a worm without user action - are at their lowest levels since 2005. SC Magazine

Full Story :

http://www.scmagazineus.com/critical-microsoft-security-bugs-at-lowest-level-since-2005/article/219312/?utm_source=

New Vulnerabilities Tested in SecureScout

• 19677 Mozilla Firefox Direct2D (aka D2D) API vulnerability

Mozilla Firefox 4.x through 5 when the Direct2D (aka D2D) API is used on Windows, allows remote attackers to bypass the Same Origin Policy, and obtain sensitive image data from a different domain, by inserting this data into a canvas.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=655836

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-31.html>

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

CVE Reference:

CVE-2011-2986 (cve.mitre.org, nvd.nist.gov)

• 19678 Mozilla Firefox Almost Native Graphics Layer Engine (ANGLE) vulnerability

Heap-based buffer overflow in Almost Native Graphics Layer Engine (ANGLE), as used in the WebGL implementation in Mozilla Firefox 4.x through 5 might allow remote attackers to execute arbitrary code via unspecified vectors.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=665934

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-31.html>

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

CVE Reference:

CVE-2011-2987 (cve.mitre.org, nvd.nist.gov)

• 19679 Mozilla Firefox WebGL shader implementation vulnerability

Buffer overflow in an unspecified string class in the WebGL shader implementation in Mozilla Firefox 4.x through 5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a long source-code block for a shader.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=665936

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-31.html>

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

CVE Reference:

CVE-2011-2988 (cve.mitre.org, nvd.nist.gov)

• 19680 Mozilla Firefox WebGL shader implementation vulnerability (CVE-2011-2989)

Buffer overflow in an unspecified string class in the WebGL shader implementation in Mozilla Firefox 4.x through 5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a long source-code block for a shader.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=665936

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-31.html>

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

CVE Reference:

CVE-2011-2989 (cve.mitre.org, nvd.nist.gov)

• 19681 Mozilla Firefox proxy-authorization credentials vulnerability

The implementation of Content Security Policy (CSP) violation reports in Mozilla Firefox 4.x through 5 does not remove proxy-authorization credentials from the listed request headers, which allows attackers to obtain sensitive information by reading a report, related to incorrect host resolution that occurs with certain redirects.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=664983

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=679588

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

CVE Reference:

CVE-2011-2990 (cve.mitre.org, nvd.nist.gov)

• 19682 Mozilla Firefox JavaScript implementation vulnerability

The browser engine in Mozilla Firefox 4.x through 5 does not properly implement JavaScript, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=655660

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-31.html>

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

CVE Reference:

CVE-2011-2991 (cve.mitre.org, nvd.nist.gov)

• 19683 Mozilla Firefox Ogg reader vulnerability

The Ogg reader in the browser engine in Mozilla Firefox 4.x through 5 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=672789

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-31.html>

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

CVE Reference:

CVE-2011-2992 (cve.mitre.org, nvd.nist.gov)

• 19684 Adobe Acrobat / Reader U3D component DOS Vulnerability

Unspecified vulnerability in the U3D component in Adobe Reader and Acrobat 10.1.1 and earlier on Windows allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, as exploited in the wild in December 2011.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/advisories/apsa11-04.html>

* BID: 50922

<http://www.securityfocus.com/bid/50922>

* URL: adobe-reader-0-day-notes-cve-2011-2462.html

<http://www.threatgeek.com/2011/12/adobe-reader-0-day-notes-cve-2011-2462.html>

CVE Reference:

CVE-2011-2462 (cve.mitre.org, nvd.nist.gov)

• 19685 Mozilla Firefox multiple unspecified vulnerability (CVE-2011-2995)

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.23 and 4.x through 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-2011-2995 (cve.mitre.org, nvd.nist.gov)

• 19686 Mozilla Firefox Unspecified vulnerability in the plugin API

Unspecified vulnerability in the plugin API in Mozilla Firefox 3.6.x before 3.6.23 allows 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=555018
- * 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>

CVE Reference:

CVE-2011-2996 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-3411 Microsoft CVSS 2.0 Score = 9.3

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: Vulnerability Impact: Risk: **High**

References:

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

CVE Reference: [CVE-2011-3411](http://cve.mitre.org/cve/2011/3411)

• CVE-2011-3410 Microsoft CVSS 2.0 Score = 9.3

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: Vulnerability Impact: Risk: **High**

References:

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

CVE Reference: [CVE-2011-3410](http://cve.mitre.org/cve/2011/3410)

• CVE-2011-3396 Microsoft CVSS 2.0 Score = 9.3

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." Per: <http://cwe.mitre.org/data/definitions/426.html> 'CWE-426: Untrusted Search Path'

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

References:

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

CVE Reference: [CVE-2011-3396](http://cve.mitre.org/cve/2011/3396)

• CVE-2011-2019 Microsoft CVSS 2.0 Score = 9.3

Untrusted search path vulnerability in Microsoft Internet Explorer 9 on Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and 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." Per: <http://technet.microsoft.com/en-us/security/bulletin/ms11-099> 'FAQ for Internet Explorer Insecure Library Loading Vulnerability - CVE-2011-2019 What is the scope of the vulnerability? This is a remote code execution vulnerability. 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.' Per: <http://cwe.mitre.org/data/definitions/426.html>

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

References:

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

CVE Reference: [CVE-2011-2019](#)

• **CVE-2011-3401 Microsoft CVSS 2.0 Score = 9.3**

ENCDEC.DLL in Windows Media Player and Media Center in Microsoft Windows XP SP2 and SP3, Windows Vista SP2, and Windows 7 Gold and 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: Vulnerability Impact: Risk: **High**

References:

MS: <http://technet.microsoft.com/security/bulletin/MS11-092>

CVE Reference: [CVE-2011-3401](#)

• **CVE-2011-3403 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Excel 2003 SP3 and Office 2004 for Mac 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: Vulnerability Impact: Risk: **High**

References:

MS: <http://technet.microsoft.com/security/bulletin/MS11-096>

CVE Reference: [CVE-2011-3403](#)

• **CVE-2011-3400 Microsoft CVSS 2.0 Score = 9.3**

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: Vulnerability Impact: Risk: **High**

References:

MS: <http://technet.microsoft.com/security/bulletin/MS11-093>

CVE Reference: [CVE-2011-3400](#)

• **CVE-2011-3397 Microsoft CVSS 2.0 Score = 9.3**

The Microsoft Time component in DATIME.DLL in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted web site that leverages an unspecified "binary behavior" in Internet Explorer, aka "Microsoft Time Remote Code Execution Vulnerability."

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

References:

MS: <http://technet.microsoft.com/security/bulletin/MS11-090>

CVE Reference: [CVE-2011-3397](#)

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