

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

Many hacks against Verisign. Wordpress users under attack. Facebook sues offender. HTC Wi-Fi codes unsecure.

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

• Security breaches impacting VeriSign emerge in filing

VeriSign, the company that manages more than 100 million .com, .net and .gov domains, was hacked numerous times in 2010, and the intruders got away with unspecified data.

The breaches, reported Thursday in a Reuters story, were acknowledged by VeriSign in a recent filing with the U.S. Securities and Exchange Commission (SEC). VeriSign compiled the filing amid new SEC guidance issued in October.

"In 2010, the company faced several successful attacks against its corporate network in which access was gained to information on a small portion of our computers and servers," the filing said. "We have investigated and do not believe these attacks breached the servers that support our domain name system (DNS) network. Information stored on the compromised corporate systems was exfiltrated." SC Magazine

Full Story :

http://www.scmagazine.com/security-breaches-impacting-verisign-emerge-in-filing/article/226029/?utm_source=feed

• WordPress attacks try to infect users with dangerous rootkit

The number of WordPress blogs that have been compromised to hurl malware onto the machines of unsuspecting users is gradually growing, security researchers said this week.

The attacks are taking advantage of website owners who are hosting an older -- and vulnerable -- version of WordPress, 3.2.1, which was updated in December but is still widely in use.

Attackers are using automated scanners to find vulnerable sites, then they are taking advantage of input validation errors to embed IFRAMES, which redirect users to exploit sites, all behind-the-scenes without the victim even noticing. SC Magazine

Full Story :

http://www.scmagazine.com/wordpress-attacks-try-to-infect-users-with-dangerous-rootkit/article/225857/?utm_source=feed

• Facebook sues Adscend Media for malware and spam

Facebook and the state of Washington have filed separate lawsuits against West Virginia-based Adscend Media LLC, alleging the company was responsible for spreading malware through Facebook and for stealing personal information from users of the social networking site.

The suits, filed in U.S. district courts in Santa Clara, Calif., and Seattle, respectively, contend that the defendants operated an advertising network that misled users into clicking on links that they thought would deliver certain types of content, such as videos or surveys, but instead installed malware on their systems and stole private information. The suits also claim that Adscend was aware and encouraged its affiliates to engage in this activity.

The Washington suit also alleges that the activity violates the state's Commercial Electronic Mail Act (CEMA) because Adscend aided its affiliates. SC Magazine

Full Story :

http://www.scmagazine.com/facebook-sues-adscend-media-for-malware-and-spam/article/225344/?utm_source=feed

• Attacks could steal HTC Wi-Fi codes with malicious app

Some HTC mobile devices, running on the Android operating system, contain a software bug that could allow attackers to steal a user's Wi-Fi credentials and network name, known as an SSID.

According to a vulnerability note posted Wednesday by US-CERT, the flaw can be exploited if users have installed applications on affected phones that contain certain permissions.

"There is an issue in certain HTC builds of Android that can expose the user's 802.1X password to any program with the 'android.permission.ACCESS_WIFI_STATE' permission," wrote researcher Bret Jordan, who discovered the weakness with Chris Hessing. "When paired with the 'android.permission.INTERNET' permission, an app could easily send usernames and passwords to a remote server for collection." SC Magazine

Full Story :

http://www.scmagazine.com/attacks-could-steal-htc-wi-fi-codes-with-malicious-app/article/226073/?utm_source=feed

New Vulnerabilities Tested in SecureScout

• 19738 Mozilla Firefox multiple memory-corruption vulnerability (CVE-2010-3175)

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.6.x before 3.6.11 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/2010/mfsa2010-64.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=554670

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=590116

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=590291

* CONFIRM:

http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_mozilla_firefox

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100120156>

* FEDORA: FEDORA-2010-16885
<http://lists.fedoraproject.org/pipermail/package-announce/2010-October/050154.html>
* FEDORA: FEDORA-2010-16897
<http://lists.fedoraproject.org/pipermail/package-announce/2010-October/050077.html>
* MANDRIVA: MDVSA-2010:210
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>
* MANDRIVA: MDVSA-2010:211
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>
* REDHAT: RHSA-2010:0782
<http://www.redhat.com/support/errata/RHSA-2010-0782.html>
* REDHAT: RHSA-2010:0861
<http://www.redhat.com/support/errata/RHSA-2010-0861.html>
* REDHAT: RHSA-2010:0896
<http://www.redhat.com/support/errata/RHSA-2010-0896.html>
* UBUNTU: USN-997-1
<http://www.ubuntu.com/usn/USN-997-1>
* UBUNTU: USN-998-1
<http://www.ubuntu.com/usn/USN-998-1>
* BID: 44245
<http://www.securityfocus.com/bid/44245>
* OVAL: oval:org.mitre.oval:def:11943
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11943>
* SECUNIA: 42867
<http://secunia.com/advisories/42867>
* VUPEN: ADV-2011-0061
<http://www.vupen.com/english/advisories/2011/0061>

CVE Reference:

CVE-2010-3175 (cve.mitre.org, nvd.nist.gov)

• 19739 Mozilla Firefox memory-corruption vulnerability (CVE-2010-3174)

Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.14 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/2010/mfsa2010-64.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=476547
* DEBIAN: DSA-2124
<http://www.debian.org/security/2010/dsa-2124>
* MANDRIVA: MDVSA-2010:210
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>
* MANDRIVA: MDVSA-2010:211
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>
* OVAL: oval:org.mitre.oval:def:11517
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11517>

CVE Reference:

CVE-2010-3174 (cve.mitre.org, nvd.nist.gov)

• 19740 Mozilla Firefox multiple memory-corruption vulnerability (CVE-2010-3176)

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.14 and 3.6.x before 3.6.11 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/2010/mfsa2010-64.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=509075
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=559344

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=566141

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=568073

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=568303

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=580151

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=583957

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=594760

* CONFIRM:
http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_mozilla_firefox

* CONFIRM:
<http://support.avaya.com/css/P8/documents/100114250>

* CONFIRM:
<http://support.avaya.com/css/P8/documents/100120156>

* DEBIAN: DSA-2124
<http://www.debian.org/security/2010/dsa-2124>

* FEDORA: FEDORA-2010-16885
<http://lists.fedoraproject.org/pipermail/package-announce/2010-October/050154.html>

* FEDORA: FEDORA-2010-16897
<http://lists.fedoraproject.org/pipermail/package-announce/2010-October/050077.html>

* MANDRIVA: MDVSA-2010:210
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:210>

* MANDRIVA: MDVSA-2010:211
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:211>

* REDHAT: RHSA-2010:0781
<http://www.redhat.com/support/errata/RHSA-2010-0781.html>

* REDHAT: RHSA-2010:0782
<http://www.redhat.com/support/errata/RHSA-2010-0782.html>

* REDHAT: RHSA-2010:0780
<http://www.redhat.com/support/errata/RHSA-2010-0780.html>

* REDHAT: RHSA-2010:0861
<http://www.redhat.com/support/errata/RHSA-2010-0861.html>

* REDHAT: RHSA-2010:0896
<http://www.redhat.com/support/errata/RHSA-2010-0896.html>

* UBUNTU: USN-997-1
<http://www.ubuntu.com/usn/USN-997-1>

* UBUNTU: USN-998-1
<http://www.ubuntu.com/usn/USN-998-1>

* BID: 44243
<http://www.securityfocus.com/bid/44243>

* OVAL: oval:org.mitre.oval:def:12132
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12132>

* SECUNIA: 42867
<http://secunia.com/advisories/42867>

* VUPEN: ADV-2011-0061
<http://www.vupen.com/english/advisories/2011/0061>

CVE Reference:

CVE-2010-3176 (cve.mitre.org, nvd.nist.gov)

• 19741 Mozilla Firefox 'nsTreeContentView' remote code execution vulnerability (CVE-2010-3167)

The nsTreeContentView function in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9 does not properly handle node removal in XUL trees, which allows remote attackers to execute arbitrary code via vectors involving access to deleted memory, related to a "dangling pointer vulnerability."

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

References:

* MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-10-171/>

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-56.html>

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=576070

* CONFIRM:
http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_mozilla_firefox
* CONFIRM:
<http://support.avaya.com/css/P8/documents/100110210>
* CONFIRM:
<http://support.avaya.com/css/P8/documents/100112690>
* DEBIAN: DSA-2106
<http://www.debian.org/security/2010/dsa-2106>
* FEDORA: FEDORA-2010-14362
<http://lists.fedoraproject.org/pipermail/package-announce/2010-September/047282.html>
* MANDRIVA: MDVSA-2010:173
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:173>
* SUSE: SUSE-SA:2010:049
<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00002.html>
* BID: 43097
<http://www.securityfocus.com/bid/43097>
* OVAL: oval:org.mitre.oval:def:12136
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12136>
* SECUNIA: 42867
<http://secunia.com/advisories/42867>
* VUPEN: ADV-2010-2323
<http://www.vupen.com/english/advisories/2010/2323>
* VUPEN: ADV-2011-0061
<http://www.vupen.com/english/advisories/2011/0061>
* XF: mozilla-nstreecontentview-code-execution(61661)
<http://xforce.iss.net/xforce/xfdb/61661>

CVE Reference:

CVE-2010-3167 (cve.mitre.org, nvd.nist.gov)

• 19742 Mozilla Firefox transform text heap buffer overflow vulnerability (CVE-2010-3166)

Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9 might allow remote attackers to execute arbitrary code.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-53.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=579655
* CONFIRM:
http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_mozilla_firefox
* CONFIRM:
<http://support.avaya.com/css/P8/documents/100112690>
* FEDORA: FEDORA-2010-14362
<http://lists.fedoraproject.org/pipermail/package-announce/2010-September/047282.html>
* MANDRIVA: MDVSA-2010:173
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:173>
* SUSE: SUSE-SA:2010:049
<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00002.html>
* BID: 43102
<http://www.securityfocus.com/bid/43102>
* OVAL: oval:org.mitre.oval:def:12186
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12186>
* SECUNIA: 42867
<http://secunia.com/advisories/42867>
* VUPEN: ADV-2010-2323
<http://www.vupen.com/english/advisories/2010/2323>
* VUPEN: ADV-2011-0061
<http://www.vupen.com/english/advisories/2011/0061>

CVE Reference:

CVE-2010-3166 (cve.mitre.org, nvd.nist.gov)

• 19743 Mozilla Firefox plugin parameters buffer overflow vulnerability (CVE-2010-1214)

Integer overflow in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7 allows remote attackers to execute arbitrary code via plugin content with many parameter elements.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-37.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=572985
- * OVAL: oval:org.mitre.oval:def:11685
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11685>

CVE Reference:

CVE-2010-1214 (cve.mitre.org, nvd.nist.gov)

• **19744 Mozilla Firefox protection mechanism vulnerability (CVE-2010-1585)**

The nsIScriptableUnescapeHTML.parseFragment method in the ParanoidFragmentSink protection mechanism in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14 does not properly sanitize HTML in a chrome document, which makes it easier for remote attackers to execute arbitrary JavaScript with chrome privileges via a javascript.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-37.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=572985
- * OVAL: oval:org.mitre.oval:def:11685
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11685>

CVE Reference:

CVE-2010-1585 (cve.mitre.org, nvd.nist.gov)

• **19745 Mozilla Firefox 'jstracer.cpp' memory corruption vulnerability (CVE-2010-1203)**

The JavaScript engine in Mozilla Firefox 3.6.x before 3.6.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors that trigger an assertion failure in jstracer.cpp.

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

References:

NULL

CVE Reference:

CVE-2010-1203 (cve.mitre.org, nvd.nist.gov)

• **19746 Mozilla Firefox JavaScript engine vulnerability (CVE-2010-1202)**

Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4 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/2010/mfsa2010-26.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=424558
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=526449
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=561031
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=561592
- * CONFIRM:
<http://support.avaya.com/css/P8/documents/100091069>
- * MANDRIVA: MDVSA-2010:125
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:125>

* REDHAT: RHSA-2010:0500
<http://www.redhat.com/support/errata/RHSA-2010-0500.html>
* REDHAT: RHSA-2010:0501
<http://www.redhat.com/support/errata/RHSA-2010-0501.html>
* SUSE: SUSE-SA:2010:030
<http://lists.opensuse.org/opensuse-security-announce/2010-07/msg00005.html>
* UBUNTU: USN-930-1
<http://ubuntu.com/usn/usn-930-1>
* UBUNTU: USN-930-2
<http://www.ubuntu.com/usn/usn-930-2>
* BID: 41050
<http://www.securityfocus.com/bid/41050>
* BID: 41094
<http://www.securityfocus.com/bid/41094>
* OVAL: oval:org.mitre.oval:def:10889
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10889>
* SECTRACK: 1024138
<http://www.securitytracker.com/id?1024138>
* SECTRACK: 1024139
<http://www.securitytracker.com/id?1024139>
* SECUNIA: 40323
<http://secunia.com/advisories/40323>
* SECUNIA: 40326
<http://secunia.com/advisories/40326>
* SECUNIA: 40401
<http://secunia.com/advisories/40401>
* SECUNIA: 40481
<http://secunia.com/advisories/40481>
* VUPEN: ADV-2010-1551
<http://www.vupen.com/english/advisories/2010/1551>
* VUPEN: ADV-2010-1557
<http://www.vupen.com/english/advisories/2010/1557>
* VUPEN: ADV-2010-1640
<http://www.vupen.com/english/advisories/2010/1640>
* VUPEN: ADV-2010-1773
<http://www.vupen.com/english/advisories/2010/1773>
* XF: firefox-javascript-ce(59661)
<http://xforce.iss.net/xforce/xfdb/59661>

CVE Reference:

CVE-2010-1202 (cve.mitre.org, nvd.nist.gov)

• 19747 Mozilla Firefox memory corruption vulnerability (CVE-2010-1201)

Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.10 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:

NULL

CVE Reference:

CVE-2010-1201 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-4562 Microsoft CVSS 2.0 Score = 4.3

Microsoft Windows 2008, 7, Vista, 2003, 2000, and XP, when using IPv6, allows remote attackers to determine whether a host is sniffing the network by sending an ICMPv6 Echo Request to a multicast address and determining whether an Echo Reply is sent, as demonstrated by thcping. NOTE: due to a typo, some sources map CVE-2010-4562 to a ProFTPD mod_sql vulnerability, but that issue is covered by CVE-2010-4652.

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

References:

FULLDISC: <http://seclists.org/fulldisclosure/2011/Apr/254>

MLIST: <http://seclists.org/dailydave/2011/q2/25>

CVE Reference: [CVE-2010-4562](#)

• **CVE-2011-4791 HP CVSS 2.0 Score = 10.0**

DBServer.exe in HP Data Protector Media Operations 6.11 and earlier allows remote attackers to execute arbitrary code via a crafted request containing a large value in a length field.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-112/>

HP: <http://www.securityfocus.com/archive/1/521472>

HP: <http://www.securityfocus.com/archive/1/521472>

CVE Reference: [CVE-2011-4791](#)

• **CVE-2011-4790 HP CVSS 2.0 Score = 9.3**

Unspecified vulnerability in HP Network Automation 7.5x, 7.6x, 9.0, and 9.10 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

SECTRAK: <http://securitytracker.com/id?1026601>

SECUNIA: <http://secunia.com/advisories/47826>

SECUNIA: <http://secunia.com/advisories/47738>

HP: http://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03171149

HP: http://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03171149

CVE Reference: [CVE-2011-4790](#)

• **CVE-2012-0449 Mozilla CVSS 2.0 Score = 10.0**

Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a malformed XSLT stylesheet that is embedded in a document.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=702466

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=701806

CONFIRM: <http://www.mozilla.org/security/announce/2012/mfsa2012-08.html>

CVE Reference: [CVE-2012-0449](#)

• **CVE-2012-0442 Mozilla CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 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: Vulnerability Impact: Risk: **High**

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=705347

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=693399

CONFIRM: <http://www.mozilla.org/security/announce/2012/mfsa2012-01.html>

CVE Reference: [CVE-2012-0442](#)

• **CVE-2012-0444 Mozilla CVSS 2.0 Score = 10.0**

Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 do not properly initialize nsChildView data structures, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted Ogg Vorbis file.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=719612

CONFIRM: <http://www.mozilla.org/security/announce/2012/mfsa2012-07.html>

CVE Reference: [CVE-2012-0444](#)

• **CVE-2012-0443 Mozilla CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 9.0, Thunderbird 5.0 through 9.0, and SeaMonkey before 2.7 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: Vulnerability Impact: Risk: **High**

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=715662

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=714600

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=713209

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=712289

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=712169

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=711651

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=707051

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=696748

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=695076

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=692817

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=684938

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=665578

CONFIRM: <http://www.mozilla.org/security/announce/2012/mfsa2012-01.html>

CVE Reference: [CVE-2012-0443](#)

• **CVE-2011-3659 Mozilla CVSS 2.0 Score = 10.0**

Use-after-free vulnerability in Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 might allow remote attackers to execute arbitrary code via vectors related to incorrect AttributeChildRemoved notifications that affect access to removed nsDOMAttribute child nodes.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=708198

CONFIRM: <http://www.mozilla.org/security/announce/2012/mfsa2012-04.html>

CVE Reference: [CVE-2011-3659](#)

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