

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

[WinHoneyd v1.5c](#) - Download WinHoneyd executable package by filling our download form. Size: 2407KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winhoneyd-1.5c.zip>

This Week in Review

Not a nice record to hold. ISPs ready to obtain user accept before tracking internet usage. Users should learn to say no. New secure software certificate.

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

• U.S.-based computers launch most cyberattacks

Computers in the United States launched the most cyberattacks in 2008, more than doubling the number from any other country, according to data published by SecureWorks, a security-as-a-service provider.

Between January and September 2008, 20.6 million attempted attacks against SecureWorks' clients originated from computers within the United States. The second-highest number of cyberattacks came from China with 7.7 million attempted attacks originating from computers there.

"We have a lot of different countries now that have joined the big leagues," Jackson said.

SC Magazine

Full Story :

<http://www.scmagazineus.com/US-based-computers-launch-most-cyberattacks/article/118270/>

• ISPs endorse user opt-in on Web tracking, deflect calls for privacy laws

September 25, 2008 (IDG News Service) WASHINGTON — Three of the four largest Internet service providers in the U.S. promised today that they will adopt policies requiring them to get meaningful permission from customers before tracking their online activities for targeted advertising purposes.

Despite a flurry of concerns that have been raised in recent months about ISPs tracking the online activities of their subscribers, Congress should give the industry time to develop a set of best practices for behavioral advertising and data collection, said Tom Tauke, executive vice president of public affairs, policy and communications at Verizon Communications Inc.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115612&source=rss_topic1

• **Computer users overeager to click popup 'OKs'**

September 25, 2008 (IDG News Service) Web surfers have a standard reaction to error messages that pop up in their Web browsers, according to new research published this week: They click "OK" and hope it will disappear. Psychologists at North Carolina State University found that computer users have a hard time distinguishing between fake Windows warning messages and the real thing. In an experiment that tested the responses of 42 Web-browsing university students, they found that almost two-thirds of them -- 63% -- would click "OK" whenever they saw a popup warning, whether it was fake or not. "Many people fall for this style of attack by not recognizing the visual elements that separate real and fake warning windows," the researchers concluded in a paper delivered at an academic conference in New York this week. That's bad news, security experts say, because fake popup messages can take you to some very bad places on the Internet. In the experiment, users tended to see the popup windows as an irritant that they needed to get rid of as quickly as possible, said Mike Wogalter, a psychology professor at North Carolina State who co-authored the study. "They really didn't think about it at all," he said. Clicking on a fake popup window can take you to a Web site you may not have intended to visit, but there can be nastier results as well. In one well-known scam, victims are sent an e-mail with a link to a Web page that promises an interesting video clip. When they try to watch it, however, a popup message tells them they need to install special codec software to view the video. In fact, the software is a Trojan downloader that then laces the victim's computer with malicious software such as keyloggers that track usernames and passwords. To make matters worse, fake popups are increasingly found on legitimate Web sites, often delivered via online advertising networks, said Eric Howes, director of malware research at security vendor Sunbelt Software. "It's becoming a real problem, because a few years ago, you would only see these fake popups on some of the seedier places on the Internet." Harvard assistant professor Ben Edelman agrees that deceptive popups are a big problem. "These are widespread, particularly when you stop one notch below the very fanciest news sites," he said. "If you go to MySpace or if you just run Google searches and click on results, you're likely to stumble on such ads." While it's easy to blame users for missing bogus error messages, Wogalter said software developers who have overwhelmed their users with too many warning messages should also share the blame. "They shouldn't be putting people into this sort of position," he said. The North Carolina State researchers said that their subjects chose the best course of action -- clicking the red X "close window" button at the top right corner to close their fake popups -- just under a third of the time. But Sunbelt's Howes said scammers are so clever these days that the "close window" buttons are often fake too. "You can get into this sort of 'Alice in Wonderland' desktop where nothing responds like you think it should," he said. Users who are really concerned about a popup message should close the window from the Windows taskbar at the bottom of the screen. Or some may feel compelled to take more drastic action. "Sometimes the safest thing to do is to kill the entire browser," Howes said.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115540&source=rss_topic1

• **New certification to stress software lifecycle safety**

The movement to create secure software received a boost with the launch of a new certification from (ISC)², a nonprofit leader in educating and certifying information security professionals.

The certification program takes a holistic approach to software security. It is code-language neutral, and applicable to anyone involved in software lifecycles. It's designed for non-technical staffers such as software architects, project managers, analysts, quality assurance testers, etc., to help eliminate code vulnerable to hacker attacks.

"The CSSLP will be a key component in better critical infrastructure protection, reducing the risk of software malpractice suits and enabling stricter adherence to industry and government regulations," added W. Hord Tipton, executive director for (ISC)².

SC Magazine

Full Story :

<http://www.scmagazineus.com/New-certification-to-stress-software-lifecycle-safety/article/118410/>

New Vulnerabilities Tested in SecureScout

• 18128 QuickTime maliciously crafted QTVR movie file, application termination and arbitrary code execution Vulnerability (CVE-2008-3625) (Remote File Checking)

A stack buffer overflow exists in QuickTime's handling of panorama atoms in QTVR (QuickTime Virtual Reality) movie files. Viewing a maliciously crafted QTVR file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue through improved bounds checking of panorama atoms.

The issue has been fixed in version 7.5.5.

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

References:

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-058/>

* CONFIRM:

<http://support.apple.com/kb/HT3027>

* APPLE: APPLE-SA-2008-09-09

<http://lists.apple.com/archives/security-announce//2008/Sep/msg00000.html>

* BID: 31086

<http://www.securityfocus.com/bid/31086>

* SECTRACK: 1020841

<http://securitytracker.com/id?1020841>

CVE Reference:

CVE-2008-3625 (cve.mitre.org, nvd.nist.gov)

• 18129 QuickTime maliciously crafted PICT image, application termination and arbitrary code execution Vulnerability (Remote File Checking)

An integer overflow exists in QuickTime's handling of PICT images. Opening a maliciously crafted PICT image may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by performing additional validation of PICT images.

The issue has been fixed in version 7.5.5.

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

References:

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-058/>

* CONFIRM:

<http://support.apple.com/kb/HT3027>

* APPLE: APPLE-SA-2008-09-09

<http://lists.apple.com/archives/security-announce//2008/Sep/msg00000.html>

* BID: 31086

<http://www.securityfocus.com/bid/31086>

* SECTRACK: 1020841

<http://securitytracker.com/id?1020841>

CVE Reference:

CVE-2008-3614 (cve.mitre.org, nvd.nist.gov)

• 18130 QuickTime handling of STSZ atoms in movie files, application termination and arbitrary code execution Vulnerability (Remote File Checking)

A memory corruption issue exists in QuickTime's handling of STSZ atoms in movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue through improved bounds checking of STSZ atoms.

The issue has been fixed in version 7.5.5.

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

References:

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-059/>

* CONFIRM:

<http://support.apple.com/kb/HT3027>

* APPLE: APPLE-SA-2008-09-09

<http://lists.apple.com/archives/security-announce//2008/Sep/msg00000.html>

* BID: 31086

<http://www.securityfocus.com/bid/31086>

* SECTRACK: 1020841

<http://securitytracker.com/id?1020841>

CVE Reference:

CVE-2008-3626 (cve.mitre.org, nvd.nist.gov)

• 18131 QuickTime handling of H.264 encoded movie files, application termination and arbitrary code execution Vulnerability (Remote File Checking)

Multiple memory corruption exist in QuickTime's handling of H.264 encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by performing additional validation of H.264 encoded movie files.

The issue has been fixed in version 7.5.5.

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

References:

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-060/>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-061/>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-062/>

* CONFIRM:

<http://support.apple.com/kb/HT3027>

* APPLE: APPLE-SA-2008-09-09

<http://lists.apple.com/archives/security-announce//2008/Sep/msg00000.html>

* BID: 31086

<http://www.securityfocus.com/bid/31086>

* SECTRACK: 1020841

<http://securitytracker.com/id?1020841>

CVE Reference:

CVE-2008-3627 (cve.mitre.org, nvd.nist.gov)

• 18132 QuickTime maliciously crafted PICT image, application termination and arbitrary code execution Vulnerability (CVE-2008-3628) (Remote File Checking)

An invalid pointer issue exists in QuickTime's handling of PICT images. Opening a maliciously crafted PICT image may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by correctly saving and restoring a global variable. This issue does not affect systems running Mac OS X.

The issue has been fixed in version 7.5.5.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT3027>

* APPLE: APPLE-SA-2008-09-09

<http://lists.apple.com/archives/security-announce//2008/Sep/msg00000.html>

* BID: 31086

<http://www.securityfocus.com/bid/31086>

* SECTRACK: 1020841

<http://securitytracker.com/id?1020841>

CVE Reference:

CVE-2008-3628 (cve.mitre.org, nvd.nist.gov)

• 18133 QuickTime maliciously crafted PICT image, application termination and arbitrary code execution Vulnerability (CVE-2008-3629) (Remote File Checking)

An out-of-bounds read issue exists in QuickTime's handling of PICT images. Opening a maliciously crafted PICT image may lead to an unexpected application termination. This update addresses the issue by performing additional validation of PICT images.

The issue has been fixed in version 7.5.5.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3027>
- * APPLE: APPLE-SA-2008-09-09
<http://lists.apple.com/archives/security-announce/2008/Sep/msg00000.html>
- * BID: 31086
<http://www.securityfocus.com/bid/31086>
- * SECTRACK: 1020841
<http://securitytracker.com/id?1020841>

CVE Reference:

CVE-2008-3629 (cve.mitre.org, nvd.nist.gov)

• 18135 Wireshark could crash while reassembling packets (Remote File Checking)

It may be possible to make Wireshark crash by injecting a series of malformed packets onto the wire or by convincing someone to read a malformed packet trace file.

The vulnerability is reported in versions 0.8.19 up to and including 1.0.1.

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

References:

- * BUGTRAQ: 20080729 rPSA-2008-0237-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/494859/100/0/threaded>
- * CONFIRM:
<http://anonsvn.wireshark.org/viewvc/index.py?view=rev&revision=25343>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2008-04.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=2470
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=454984
- * CONFIRM:
<http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0237>
- * CONFIRM:
<https://issues.rpath.com/browse/RPL-2684>
- * FEDORA: FEDORA-2008-6440
<https://www.redhat.com/archives/fedora-package-announce/2008-July/msg00544.html>
- * GENTOO: GLSA-200808-04
<http://security.gentoo.org/glsa/glsa-200808-04.xml>
- * MANDRIVA: MDVSA-2008:152
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:152>
- * SUSE: SUSE-SR:2008:017
<http://lists.opensuse.org/opensuse-security-announce/2008-08/msg00006.html>
- * BID: 30181
<http://www.securityfocus.com/bid/30181>
- * FRSIRT: ADV-2008-2057
<http://www.frsirt.com/english/advisories/2008/2057/references>
- * SECTRACK: 1020471
<http://securitytracker.com/id?1020471>
- * SECUNIA: 31044
<http://secunia.com/advisories/31044>
- * SECUNIA: 31085
<http://secunia.com/advisories/31085>
- * SECUNIA: 31257
<http://secunia.com/advisories/31257>
- * SECUNIA: 31378
<http://secunia.com/advisories/31378>
- * SECUNIA: 31687
<http://secunia.com/advisories/31687>

* XF: wireshark-packets-dos(43719)
<http://xforce.iss.net/xforce/xfdb/43719>

CVE Reference:

CVE-2008-3145 (cve.mitre.org, nvd.nist.gov)

• 18136 Wireshark NCP dissector buffer overflows and denial of service Vulnerabilities (Remote File Checking)

Multiple buffer overflows in packet_ncp2222.inc in Wireshark (formerly Ethereal) 0.9.7 up to and including 1.0.2 allow attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted NCP packet that causes an invalid pointer to be used.

The vulnerability is reported in versions 0.9.7 up to and including 1.0.2.

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

References:

- * BUGTRAQ: 20080917 rPSA-2008-0278-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/496487/100/0/threaded>
- * CONFIRM:
<http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0278>
- * SUSE: SUSE-SR:2008:017
<http://lists.opensuse.org/opensuse-security-announce/2008-08/msg00006.html>
- * CONFIRM:
http://bugs.wireshark.org/bugzilla/show_bug.cgi?id=2675
- * CONFIRM:
<http://www.wireshark.org/security/wmpa-sec-2008-05.html>
- * SECTrack: 1020819
<http://www.securitytracker.com/id?1020819>
- * SECUNIA: 31687
<http://secunia.com/advisories/31687>
- * SECUNIA: 31886
<http://secunia.com/advisories/31886>

CVE Reference:

CVE-2008-3146 (cve.mitre.org, nvd.nist.gov)

• 18137 Wireshark NCP dissector, denial of service Vulnerability (Remote File Checking)

Wireshark (formerly Ethereal) 0.9.7 up to and including 1.0.2 allows attackers to cause a denial of service (hang) via a crafted NCP packet that triggers an infinite loop.

The vulnerability is reported in versions 0.9.7 up to and including 1.0.2.

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

References:

- * BUGTRAQ: 20080917 rPSA-2008-0278-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/496487/100/0/threaded>
- * CONFIRM:
http://bugs.wireshark.org/bugzilla/show_bug.cgi?id=2675
- * CONFIRM:
<http://www.wireshark.org/security/wmpa-sec-2008-05.html>
- * CONFIRM:
<http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0278>
- * SECTrack: 1020819
<http://www.securitytracker.com/id?1020819>
- * SECUNIA: 31886
<http://secunia.com/advisories/31886>

CVE Reference:

CVE-2008-3932 (cve.mitre.org, nvd.nist.gov)

• 18138 Wireshark crafted zlib-compressed data, denial of service Vulnerability (Remote File Checking)

Wireshark (formerly Ethereal) 0.10.14 through 1.0.2 included allows attackers to cause a denial of service (crash) via a packet with crafted zlib-compressed data that triggers an invalid read in the tvb_uncompress function.

The vulnerability is reported in versions 0.10.14 up to and including 1.0.2.

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

References:

- * BUGTRAQ: 20080917 rPSA-2008-0278-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/496487/100/0/threaded>
- * MISC:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=2682
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=2649
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2008-05.html>
- * CONFIRM:
<http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0278>
- * SECTRACK: 1020819
<http://www.securitytracker.com/id?1020819>
- * SECUNIA: 31886
<http://secunia.com/advisories/31886>

CVE Reference:

CVE-2008-3933 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-0016 Mozilla CVSS 2.0 Score = 10.0

Stack-based buffer overflow in the URL parsing implementation in Mozilla Firefox before 2.0.0.17 and SeaMonkey before 1.1.12 allows remote attackers to execute arbitrary code via a crafted UTF-8 URL in a link.

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

References:

- CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=443288
- CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=451617
- BID: <http://www.securityfocus.com/bid/31397>
- CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-37.html>
- MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2008:205>
- SLACKWARE:
<http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.405232>
- SECUNIA: <http://secunia.com/advisories/32042>

CVE Reference: [CVE-2008-0016](#)

• CVE-2008-4061 Mozilla CVSS 2.0 Score = 10.0

Integer overflow in the MathML component in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via an mtd element with a large integer value in the rowspan attribute, related to the layout engine. NOTE: Thunderbird shares the browser engine with Firefox and could be vulnerable if JavaScript were to be enabled in mail. This is not the default setting and we strongly discourage users from running JavaScript in mail. Without further investigation we cannot rule out the possibility that for some of these an attacker might be able to prepare memory for exploitation through some means other than JavaScript such as large images.

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

References:

- CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=443089
- CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-42.html>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2008:205>

SLACKWARE:

<http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.405232>

SECUNIA: <http://secunia.com/advisories/32042>

CVE Reference: [CVE-2008-4061](#)

• **CVE-2008-4062 Mozilla CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the JavaScript engine and (1) misinterpretation of the characteristics of Namespace and QName in jsxml.c, (2) misuse of signed integers in the nsEscapeCount function in nsEscape.cpp, and (3) interaction of JavaScript garbage collection with certain use of an NPObj in the nsNPObjWrapper::GetNewOrUsed function in nsJSNPRuntime.cpp. NOTE: Thunderbird shares the browser engine with Firefox and could be vulnerable if JavaScript were to be enabled in mail. This is not the default setting and we strongly discourage users from running JavaScript in mail. Without further investigation we cannot rule out the possibility that for some of these an attacker might be able to prepare memory for exploitation through some means other than JavaScript such as large images.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=445229

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=444608

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=367736

CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-42.html>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2008:205>

SLACKWARE:

<http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.405232>

SECUNIA: <http://secunia.com/advisories/32042>

CVE Reference: [CVE-2008-4062](#)

• **CVE-2008-4063 Mozilla CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the layout engine and (1) a zero value of the "this" variable in the nsContentList::Item function; (2) interaction of the indic IME extension, a Hindi language selection, and the "g" character; and (3) interaction of the nsFrameList::SortByContentOrder function with a certain insufficient protection of inline frames. NOTE: Thunderbird shares the browser engine with Firefox and could be vulnerable if JavaScript were to be enabled in mail. This is not the default setting and we strongly discourage users from running JavaScript in mail. Without further investigation we cannot rule out the possibility that for some of these an attacker might be able to prepare memory for exploitation through some means other than JavaScript such as large images.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=444452

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=433758

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=413048

CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-42.html>

CVE Reference: [CVE-2008-4063](#)

• **CVE-2008-4064 Mozilla CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to graphics

rendering and (1) handling of a long alert messagebox in the `cairo_surface_set_device_offset` function, (2) integer overflows when handling animated PNG data in the `info_callback` function in `nsPNGDecoder.cpp`, and (3) an integer overflow when handling SVG data in the `nsSVGFEGaussianBlurElement::SetupPredivide` function in `nsSVGFilters.cpp`. NOTE: Thunderbird shares the browser engine with Firefox and could be vulnerable if JavaScript were to be enabled in mail. This is not the default setting and we strongly discourage users from running JavaScript in mail. Without further investigation we cannot rule out the possibility that for some of these an attacker might be able to prepare memory for exploitation through some means other than JavaScript such as large images.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=443693

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=441995

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=441368

CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-42.html>

CVE Reference: [CVE-2008-4064](#)

• **CVE-2008-3837 Mozilla CVSS 2.0 Score = 9.3**

Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, and SeaMonkey before 1.1.12, allow user-assisted remote attackers to move a window during a mouse click, and possibly force a file download or unspecified other drag-and-drop action, via a crafted onmousedown action that calls `window.moveBy`, a variant of CVE-2003-0823.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=329385

CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-40.html>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2008:205>

SLACKWARE:

<http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.405232>

SECUNIA: <http://secunia.com/advisories/32042>

CVE Reference: [CVE-2008-3837](#)

• **CVE-2008-4068 Mozilla CVSS 2.0 Score = 7.8**

Directory traversal vulnerability in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to bypass "restrictions imposed on local HTML files," and obtain sensitive information and prompt users to write this information into a file, via directory traversal sequences in a resource: URI.

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

References:

CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-44.html>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2008:205>

SLACKWARE:

<http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.405232>

SECUNIA: <http://secunia.com/advisories/32042>

CVE Reference: [CVE-2008-4068](#)

• **CVE-2008-3835 Mozilla CVSS 2.0 Score = 7.5**

The `nsXMLDocument::OnChannelRedirect` function in Mozilla Firefox before 2.0.0.17, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to bypass the Same Origin Policy and execute arbitrary JavaScript code via unknown vectors. NOTE: Thunderbird shares the browser engine with Firefox and could be vulnerable if JavaScript were to be enabled in mail. This is not the default setting and we strongly discourage users from running JavaScript in mail.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=439034

CONFIRM: <http://www.mozilla.org/security/announce/2008/mfsa2008-38.html>

MANDRIVA: <http://www.mandriva.com/security/advisories?name=MDVSA-2008:205>

SLACKWARE:

<http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.405232>

SECUNIA: <http://secunia.com/advisories/32042>

CVE Reference: [CVE-2008-3835](#)

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