

2010 Issue #20

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

This Week in Review

New botnet uses servers instead of individual PCs. About Joe Weiss and infrastructure security. Avalanche seems to slow down. MS fixing holes in Outlook and Office.

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

• Servers hacked to launch more powerful DDoS attacks

Researchers at security firm Imperva have discovered a botnet consisting of web servers, rather than individual PCs, that is being used to launch more devastating denial-of-service (DDoS) attacks.

An attacker by the name of "Exeman" has infected around 400 web servers with a simple 40-line PHP script, which includes a malicious application that can be used to launch DDoS attacks, Imperva CTO Amichai Shulman told SCMagazineUS.com on Wednesday.

The application provides a dashboard and control panel that can be used to input the URL of an intended target and configure the IP, port and duration of the attack, Shulman said. The attacker may have leveraged a common flaw, called a remote file inclusion vulnerability, to compromise the servers. SC Magazine

Full Story :

http://www.scmagazineus.com/servers-hacked-to-launch-more-powerful-ddos-attacks/article/170046/?utm_source=f

• **Critical infrastructure security crusader Joe Weiss (Q&A)**

When Joe Weiss goes to cybersecurity conferences, he rubs elbows with world dignitaries, law enforcement officials, and large corporations, but usually he's the lone representative from the industrial critical infrastructures.

He's been beating the security drumbeat for the utility industry and the others for at least 10 years, as previously isolated control systems at electrical and nuclear plants, electric substations, oil refineries, and water distribution centers are being modernized with direct connections to other systems and to the public Internet. The introduction of the smart grid is pushing old-school industrial control managers off a technological cliff and increasing the chances of problems. This is similar to the system glitch and subsequent stock plunge last week that was made possible by Wall Street's move to high-frequency trading and electronic exchanges.

Joe Weiss, security expert for the industrial critical infrastructures. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20004505-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• **"Avalanche" phishing slowing, but was all the 2009 rage**

A single crime syndicate dominated the phishing scene last year, but the outfit appears to be taking quieter breaths in 2010, a new report concludes.

The Eastern European-based ring, dubbed Avalanche, was responsible for roughly two-thirds of all phishing attacks launched in the second half of last year, according to a study released Wednesday by the nonprofit Anti-Phishing Working Group (APWG). That is up significantly from the first half of 2009, when Avalanche was blamable for a quarter of all phishes.

Specifically during the second half of last year, Avalanche accounted for 84,250 of 126,597 total phishing attacks, defined as a phishing site that targets a specific brand, the report said. The 126,597 number was more than double the amount of phishing attacks recorded during the first half of 2009. SC Magazine

Full Story :

http://www.scmagazineus.com/avalanche-phishing-slowng-but-was-all-the-2009-rage/article/170052/?utm_source=fe

• **Microsoft releases critical fixes for Windows, Office holes**

Microsoft issued two critical bulletins on Tuesday fixing holes in its e-mail programs and the Visual Basic for Applications programming language implementation built into Office.

Bulletin MS10-030 resolves a vulnerability affecting Outlook Express, Windows Mail, and Windows Live Mail that an attacker could exploit by compromising a mail server, hosting a malicious mail server, or performing a man-in-the-middle attack to intercept communications between the client and the server.

Bulletin MS10-031 fixes a hole in Microsoft Visual Basic for Applications (VBA) that could allow an attacker to remotely run code if a host application opens and passes a malicious file to the VBA runtime environment. The update resolves the problem by changing the way VBA searches for ActiveX Controls are embedded in documents. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20004694-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• **18793 Mozilla Firefox - XSS using addEventListener and setTimeout on a wrapped object Vulnerability (Remote File Checking)**

Mozilla security researcher moz_bug_r_a4 reports that by using an appropriately wrapped object it was possible to bypass the fix for MFSA 2007-19. Prior to Firefox 3.6 this gives an attacker the ability to perform cross-site scripting attacks against arbitrary sites as in the original MFSA 2007-19 attack. Due to unrelated changes in the browser engine used by Firefox 3.6, attacks in that version are limited to capturing keystroke events from a cross-origin frame or window rather than full DOM access. Those events might be sufficient to illicitly obtain passwords or other sensitive information entered into web forms.

The issue has been fixed in Firefox 3.6.2, 3.5.8, 3.0.18.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-12.html>

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=531364
* BID: 38918
<http://www.securityfocus.com/bid/38918>
* VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0171 (cve.mitre.org, nvd.nist.gov)

● **18794 Mozilla Thunderbird - Browser chrome defacement via cached XUL stylesheets Vulnerability (Remote File Checking)**

Mozilla developer Wladimir Palant reported that stylesheets used in remote XUL documents can wind up in the XUL cache where it can later be accessed by browser chrome for use in styling the user interface. A malicious website could use this issue to pollute a user's XUL cache and change style attributes of their browser such as font size and color.

The issue has been fixed in Thunderbird 3.0.2.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-14.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=535806
* BID: 38918
<http://www.securityfocus.com/bid/38918>
* VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0169 (cve.mitre.org, nvd.nist.gov)

● **18795 Mozilla Thunderbird - crashes in the browser engine Vulnerability (Remote File Checking)**

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances, and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Thunderbird 3.0.4.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-16.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=488850
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=491722
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=496011
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=499862
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=542136
* FEDORA: FEDORA-2010-5526
<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038367.html>
* FEDORA: FEDORA-2010-5539
<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038378.html>
* MANDRIVA: MDVSA-2010:070
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>
* UBUNTU: USN-921-1
<http://ubuntu.com/usn/usn-921-1>
* SECTRACK: 1023775
<http://securitytracker.com/id?1023775>
* SECTRACK: 1023781

<http://securitytracker.com/id?1023781>

* SECUNIA: 39136

<http://secunia.com/advisories/39136>

* SECUNIA: 39204

<http://secunia.com/advisories/39204>

* SECUNIA: 39242

<http://secunia.com/advisories/39242>

* SECUNIA: 39243

<http://secunia.com/advisories/39243>

* SECUNIA: 39397

<http://secunia.com/advisories/39397>

* VUPEN: ADV-2010-0748

<http://www.vupen.com/english/advisories/2010/0748>

* VUPEN: ADV-2010-0849

<http://www.vupen.com/english/advisories/2010/0849>

* XF: firefox-browser-eng-code-execution(57388)

<http://xforce.iss.net/xforce/xfdb/57388>

CVE Reference:

CVE-2010-0173 (cve.mitre.org, nvd.nist.gov)

• 18796 Mozilla Thunderbird - Remote code execution with use-after-free in nsTreeSelection Vulnerability (Remote File Checking)

Security researcher regenrecht reported via TippingPoint's Zero Day Initiative that a select event handler for XUL tree items could be called after the tree item was deleted. This results in the execution of previously freed memory which an attacker could use to crash a victim's browser and run arbitrary code on the victim's computer.

The issue has been fixed in Thunderbird 3.0.4.

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

References:

* BUGTRAQ: 20100402 ZDI-10-050: Mozilla Firefox nsTreeSelection EventListener Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/510542/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-050>

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-17.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=375928

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=540100

* DEBIAN: DSA-2027

<http://www.debian.org/security/2010/dsa-2027>

* FEDORA: FEDORA-2010-5526

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038367.html>

* FEDORA: FEDORA-2010-5539

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038378.html>

* FEDORA: FEDORA-2010-5561

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038406.html>

* MANDRIVA: MDVSA-2010:070

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>

* REDHAT: RHSA-2010:0332

<http://www.redhat.com/support/errata/RHSA-2010-0332.html>

* REDHAT: RHSA-2010:0333

<http://www.redhat.com/support/errata/RHSA-2010-0333.html>

* UBUNTU: USN-921-1

<http://ubuntu.com/usn/usn-921-1>

* SECTRACK: 1023780

<http://securitytracker.com/id?1023780>

* SECTRACK: 1023782

<http://securitytracker.com/id?1023782>

* SECUNIA: 38566

<http://secunia.com/advisories/38566>

* SECUNIA: 39117

<http://secunia.com/advisories/39117>

* SECUNIA: 39136

<http://secunia.com/advisories/39136>

* SECUNIA: 39204

<http://secunia.com/advisories/39204>

* SECUNIA: 39240

<http://secunia.com/advisories/39240>

* SECUNIA: 39242

<http://secunia.com/advisories/39242>

* SECUNIA: 39243

<http://secunia.com/advisories/39243>

* SECUNIA: 39308

<http://secunia.com/advisories/39308>

* SECUNIA: 39397

<http://secunia.com/advisories/39397>

* VUPEN: ADV-2010-0748

<http://www.vupen.com/english/advisories/2010/0748>

* VUPEN: ADV-2010-0764

<http://www.vupen.com/english/advisories/2010/0764>

* VUPEN: ADV-2010-0765

<http://www.vupen.com/english/advisories/2010/0765>

* VUPEN: ADV-2010-0781

<http://www.vupen.com/english/advisories/2010/0781>

* VUPEN: ADV-2010-0790

<http://www.vupen.com/english/advisories/2010/0790>

* VUPEN: ADV-2010-0849

<http://www.vupen.com/english/advisories/2010/0849>

* XF: firefox-nstreeselection-code-execution(57390)

<http://xforce.iss.net/xforce/xfdb/57390>

CVE Reference:

CVE-2010-0175 (cve.mitre.org, nvd.nist.gov)

• 18797 Mozilla Thunderbird - XSS using addEventListener and setTimeout on a wrapped object Vulnerability (Remote File Checking)

Mozilla security researcher moz_bug_r_a4 reports that by using an appropriately wrapped object it was possible to bypass the fix for MFSA 2007-19. Prior to Firefox 3.6 this gives an attacker the ability to perform cross-site scripting attacks against arbitrary sites as in the original MFSA 2007-19 attack. Due to unrelated changes in the browser engine used by Firefox 3.6, attacks in that version are limited to capturing keystroke events from a cross-origin frame or window rather than full DOM access. Those events might be sufficient to illicitly obtain passwords or other sensitive information entered into web forms.

The issue has been fixed in Thunderbird 3.0.2.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-12.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=531364

* BID: 38918

<http://www.securityfocus.com/bid/38918>

* VUPEN: ADV-2010-0692

<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0171 (cve.mitre.org, nvd.nist.gov)

• 18798 Mozilla Firefox - crash in the browser engine affecting Firefox 3.6 Vulnerability (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Firefox 3.6.2.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-11.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=542849
* MANDRIVA: MDVSA-2010:070
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>
* BID: 38918
<http://www.securityfocus.com/bid/38918>
* VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0165 (cve.mitre.org, nvd.nist.gov)

• 18799 Mozilla Firefox - crash in the browser engine Vulnerability (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Firefox 3.6.2, 3.5.8, 3.0.18.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-11.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=534082
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=535641
* MANDRIVA: MDVSA-2010:070
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>
* BID: 38918
<http://www.securityfocus.com/bid/38918>
* BID: 38944
<http://www.securityfocus.com/bid/38944>
* VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0167 (cve.mitre.org, nvd.nist.gov)

• 18800 Mozilla Thunderbird - crash in the browser engine affecting Firefox 3.6 Vulnerability (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Thunderbird 3.0.2.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-11.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=542849
* MANDRIVA: MDVSA-2010:070
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>
* BID: 38918
<http://www.securityfocus.com/bid/38918>
* VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0165 (cve.mitre.org, nvd.nist.gov)

• 18801 Mozilla Thunderbird - crash in the browser engine Vulnerability (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Thunderbird 3.0.2.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-11.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=534082
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=535641
- * MANDRIVA: MDVSA-2010:070
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>
- * BID: 38918
<http://www.securityfocus.com/bid/38918>
- * BID: 38944
<http://www.securityfocus.com/bid/38944>
- * VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0167 (cve.mitre.org, nvd.nist.gov)

• 18802 Mozilla Firefox - XSS via plugins and unprotected Location object Vulnerability (Remote File Checking)

Mozilla developer Blake Kaplan reported that the window.location object was made a normal overridable JavaScript object in the Firefox 3.6 browser engine (Gecko 1.9.2) because new mechanisms were developed to enforce the same-origin policy between windows and frames. This object is unfortunately also used by some plugins to determine the page origin used for access restrictions. A malicious page could override this object to fool a plugin into granting access to data on another site or the local file system. The behavior of older Firefox versions has been restored.

The issue has been fixed in Firefox 3.6.2.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-10.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=541530
- * MANDRIVA: MDVSA-2010:070
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>
- * BID: 38918
<http://www.securityfocus.com/bid/38918>
- * BID: 38919
<http://www.securityfocus.com/bid/38919>
- * VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0170 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-0815 Microsoft CVSS 2.0 Score = 9.3

VBE6.DLL in Microsoft Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Visual Basic for Applications (VBA), and VBA SDK 6.3 through 6.5 does not properly search for ActiveX controls that are embedded in documents, which allows remote attackers to execute arbitrary code via a crafted document, aka "VBE6.DLL Stack Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-031.msp>

CVE Reference: [CVE-2010-0815](#)

• **CVE-2010-0816 Microsoft CVSS 2.0 Score = 9.3**

Integer overflow in inetcomm.dll in Microsoft Outlook Express 5.5 SP2, 6, and 6 SP1; Windows Live Mail on Windows XP SP2 and SP3, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7; and Windows Mail on Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote e-mail servers and man-in-the-middle attackers to execute arbitrary code via a crafted (1) POP3 or (2) IMAP response, as demonstrated by a certain +OK response on TCP port 110, aka "Outlook Express and Windows Mail Integer Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-030.msp>

BID: <http://www.securityfocus.com/bid/40052>

MISC: http://www.protekresearchlab.com/index.php?option=com_content&view=article&id=13&Itemid=13

BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2010-05/0068.html>

CVE Reference: [CVE-2010-0816](#)

• **CVE-2010-1914 PHP CVSS 2.0 Score = 5.0**

The Zend Engine in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information by interrupting the handler for the (1) ZEND_BW_XOR opcode (shift_left_function), (2) ZEND_SL opcode (bitwise_xor_function), or (3) ZEND_SR opcode (shift_right_function), related to the convert_to_long_base function.

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

References:

MISC:

http://www.php-security.org/2010/05/08/mops-2010-016-php-zend_sr-opcode-interruption-address-information-leak-vulnerability/

MISC:

http://www.php-security.org/2010/05/08/mops-2010-015-php-zend_sl-opcode-interruption-address-information-leak-vulnerability/

MISC:

http://www.php-security.org/2010/05/08/mops-2010-014-php-zend_bw_xor-opcode-interruption-address-information-leak-vulnerability/

CVE Reference: [CVE-2010-1914](#)

• **CVE-2010-1915 PHP CVSS 2.0 Score = 5.0**

The preg_quote function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature, modification of ZVALs whose values are not updated in the associated local variables, and access of previously-freed memory.

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

References:

MISC:

http://www.php-security.org/2010/05/09/mops-2010-017-php-preg_quote-interruption-information-leak-vulnerability/index.html

CVE Reference: [CVE-2010-1915](#)

• **CVE-2010-1917 PHP CVSS 2.0 Score = 5.0**

Stack consumption vulnerability in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to cause a denial of service (PHP crash) via a crafted first argument to the fnmatch function, as demonstrated using a long string.

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

References:

MISC:

<http://www.php-security.org/2010/05/11/mops-2010-021-php-fnmatch-stack-exhaustion-vulnerability/index.html>

CVE Reference: [CVE-2010-1917](#)

• **CVE-2010-1455 Wireshark CVSS 2.0 Score = 4.3**

The DOCSIS dissector in Wireshark 0.9.6 through 1.0.12 and 1.2.0 through 1.2.7 allows user-assisted remote attackers to cause a denial of service (application crash) via a malformed packet trace file.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/1081>

CONFIRM: https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4646

CONFIRM: https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4644

CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2010-04.html>

CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2010-03.html>

BID: <http://www.securityfocus.com/bid/39950>

OSVDB: <http://www.osvdb.org/64363>

SECUNIA: <http://secunia.com/advisories/39661>

CVE Reference: [CVE-2010-1455](#)

• **CVE-2010-0730 redhat CVSS 2.0 Score = 2.6**

The MMIO instruction decoder in the Xen hypervisor in the Linux kernel 2.6.18 in Red Hat Enterprise Linux (RHEL) 5 allows guest OS users to cause a denial of service (32-bit guest OS crash) via vectors that trigger an unspecified instruction emulation. Per: <http://secunia.com/advisories/39649> 'Successful exploitation requires a 32bit system and access to an MMIO region.'

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

REDHAT: <http://www.redhat.com/support/errata/RHSA-2010-0398.html>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=572971

BID: <http://www.securityfocus.com/bid/39979>

SECUNIA: <http://secunia.com/advisories/39649>

CVE Reference: [CVE-2010-0730](#)

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