

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

Most of us fall prey. New way to stop cyber crime. Malicious pdf out there. Phishers and their targets.

New PCI rules are in effect as of September 1st and netVigilance PCI reports are, of course, updated according to the requirements.

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

- **Study: Two-thirds of Web surfers fall prey to online crime**

The average amount of time spent to resolve a cybercrime and the average cost vary from country to country, according to the Norton study.

(Credit: Symantec/Norton)

About two-thirds of Internet users globally and nearly three-quarters of Web surfers in the U.S. have been victims of online crime, according to a study to be released on Wednesday. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20015772-245.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Microsoft to assume control over Waledac domains**

The fight to dismantle the prolific Waledac botnet appears to be over, Microsoft announced Wednesday. A magistrate judge in the U.S. District Court of Eastern Virginia last week recommended the court permanently transfer ownership of the 276 domains behind Waledac to Microsoft, a move that would effectively stop the cybercriminals from ever leveraging the botnet again. The Waledac botnet is a network of tens of thousands of compromised computers used to spread malware, send spam and commit other cybercrimes.

The defendants in the case, who did not come forward in court but launched distributed denial-of-service attacks against the law firm that filed the lawsuit, have 14 days to object the latest ruling until it is deemed final, Microsoft said in a blog post Wednesday. Microsoft does not know the identities of the defendants. SC Magazine

Full Story :

http://www.scmagazineus.com/microsoft-to-assume-control-over-waledac-domains/article/178492/?utm_source=feed

• Security firm: Zero-day Adobe exploit in the wild

Security firm Trend Micro has found malicious files in the wild related to a zero-day exploit in Adobe Reader and Adobe Acrobat.

The file that Trend Micro spotted on the Web called TROJ_PIDIEF.WM includes two "downloaders" called TROJ_DLOADR.WM and TROJ_CHIFRAX.BU. According to Adobe Systems, which first mentioned the exploit Wednesday, the malicious files would allow an attacker to "take control of the affected system." The company said that it could also "cause a crash."

Trend Micro said that the site where it found the exploit was registered in Hong Kong, while the servers that host the page are in Germany and the United States. It said that "some effort was placed into hiding the actual persons responsible for this attack." Cnet Security

Full Story :

http://news.cnet.com/8301-13506_3-20015938-17.html?part=rss&subj=news&tag=2547-1_3-0-20

• A flood of phishing sites and how to avoid them

This pie chart shows the business categories targeted by phishers and their respective proportion of fake sites, according to PandaLab's latest report.

(Credit: PandaLabs)

You could call it the Web site phishing deluge. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20016026-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 18912 PHP php_mysqlnd_read_error_from_line function buffer overflow Vulnerability

The php_mysqlnd_read_error_from_line function in the Mysqlnd extension in PHP 5.3 through 5.3.2 does not properly calculate a buffer length, which allows context-dependent attackers to trigger a heap-based buffer overflow via crafted inputs that cause a negative length value to be used.

The issue has been fixed in PHP versions 5.3.3.

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

References:

* MISC:

http://php-security.org/2010/05/31/mops-2010-058-php-php_mysqlnd_read_error_from_line-buffer-overflow-vulnerability/

* CONFIRM:

http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/NEWS?r1=298701&r2=298703&pathrev=298703

* CONFIRM:

<http://svn.php.net/viewvc?view=revision&revision=298703>

CVE Reference:

CVE-2010-3063 (cve.mitre.org, nvd.nist.gov)

• 18913 PHP mysqlnd_wireprotocol buffer overflow Vulnerability

mysqlnd_wireprotocol.c in the Mysqlnd extension in PHP 5.3 through 5.3.2 allows remote attackers to (1) read sensitive memory via a modified length value, which is not properly handled by the php_mysqlnd_ok_read function; or

(2) trigger a heap-based buffer overflow via a modified length value, which is not properly handled by the `php_mysqlnd_rset_header_read` function.

The issue has been fixed in PHP versions 5.3.3.

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

References:

* MISC:

http://php-security.org/2010/05/31/mops-2010-056-php-php_mysqlnd_ok_read-information-leak-vulnerability/index.html

* MISC:

http://php-security.org/2010/05/31/mops-2010-057-php-php_mysqlnd_rset_header_read-buffer-overflow-vulnerability/index.html

* CONFIRM:

http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/NEWS?r1=298701&pathrev=298703

* CONFIRM:

<http://svn.php.net/viewvc?view=revision&revision=298703>

CVE Reference:

CVE-2010-3062 (cve.mitre.org, nvd.nist.gov)

• 18914 PHP phar extension format string Vulnerabilities

Multiple format string vulnerabilities in the phar extension in PHP 5.3 before 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted `phar://` URI that is not properly handled by the (1) `phar_stream_flush`, (2) `phar_wrapper_unlink`, (3) `phar_parse_url`, or (4) `phar_wrapper_open_url` functions in `ext/phar/stream.c`; and the (5) `phar_wrapper_open_dir` function in `ext/phar/dirstream.c`, which triggers errors in the `php_stream_wrapper_log_error` function.

The issue has been fixed in PHP versions 5.3.3.

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

References:

* MISC:

http://php-security.org/2010/05/14/mops-2010-024-php-phar_stream_flush-format-string-vulnerability/index.html

* MISC:

http://php-security.org/2010/05/14/mops-2010-025-php-phar_wrapper_open_dir-format-string-vulnerability/index.html

* MISC:

http://php-security.org/2010/05/14/mops-2010-026-php-phar_wrapper_unlink-format-string-vulnerability/index.html

* MISC:

http://php-security.org/2010/05/14/mops-2010-027-php-phar_parse_url-format-string-vulnerabilities/index.html

* MISC:

http://php-security.org/2010/05/14/mops-2010-028-php-phar_wrapper_open_url-format-string-vulnerabilities/index.html

CVE Reference:

CVE-2010-2094 (cve.mitre.org, nvd.nist.gov)

• 18915 PHP dechunk filter integer overflow Vulnerability

The dechunk filter in PHP 5.3 through 5.3.2, when decoding an HTTP chunked encoding stream, allows context-dependent attackers to cause a denial of service (crash) and possibly trigger memory corruption via a negative chunk size, which bypasses a signed comparison, related to an integer overflow in the chunk size decoder.

The issue has been fixed in PHP versions 5.3.3.

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

References:

* MISC:

<http://php-security.org/2010/05/02/mops-2010-003-php-dechunk-filter-signed-comparison-vulnerability/index.html>

* VUPEN: VUPEN/ADV-2010-1065

<http://www.vupen.com/english/advisories/2010/1065>

CVE Reference:

CVE-2010-1866 (cve.mitre.org, nvd.nist.gov)

• 18916 QuickTime heap buffer overflow exists in the handling of PICT images (Remote File Checking)

A heap buffer overflow exists in the handling of PICT images. Opening a maliciously crafted PICT image may lead to an unexpected application termination or arbitrary code execution. The issue is addressed through improved validation of PICT images.

The issue has been fixed in version 7.6.6.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT3937>
- * APPLE: APPLE-SA-2009-11-09-1
<http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>
- * APPLE: APPLE-SA-2010-03-30-1
<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>
- * BID: 36956
<http://www.securityfocus.com/bid/36956>
- * OVAL: oval:org.mitre.oval:def:6707
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6707>
- * VUPEN: ADV-2009-3184
<http://www.vupen.com/english/advisories/2009/3184>

CVE Reference:

CVE-2009-2837 (cve.mitre.org, nvd.nist.gov)

• 18917 QuickTime memory corruption issue exists in the handling of QDM2 encoded audio content (Remote File Checking)

A memory corruption issue exists in the handling of QDM2 encoded audio content. Playing maliciously crafted audio content may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved bounds checking.

The issue has been fixed in version 7.6.6.

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

References:

- * BUGTRAQ: 20100402 ZDI-10-041: Apple QuickTime QDM2/QDCA Atom Remote Code Execution Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/510517/100/0/threaded>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-10-041>
- * CONFIRM:
<http://support.apple.com/kb/HT4077>
- * APPLE: APPLE-SA-2010-03-29-1
<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>
- * APPLE: APPLE-SA-2010-03-30-1
<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>
- * OVAL: oval:org.mitre.oval:def:6922
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6922>

CVE Reference:

CVE-2010-0059 (cve.mitre.org, nvd.nist.gov)

• 18918 QuickTime memory corruption issue exists in the handling of QDMC encoded audio content (Remote File Checking)

A memory corruption issue exists in the handling of QDMC encoded audio content. Playing maliciously crafted audio content may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved bounds checking.

The issue has been fixed in version 7.6.6.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT4077>
- * APPLE: APPLE-SA-2010-03-29-1
<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>

* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>

* OVAL: oval:org.mitre.oval:def:7513

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7513>

CVE Reference:

CVE-2010-0060 (cve.mitre.org, nvd.nist.gov)

• 18919 QuickTime heap buffer overflow exists in the handling of H.263 encoded movie files (Remote File Checking)

A heap buffer overflow exists in the handling of H.263 encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by performing additional validation of H.263 encoded movie files.

The issue has been fixed in version 7.6.6.

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

References:

* BUGTRAQ: 20100402 ZDI-10-036: Apple QuickTime H.263 PictureHeader Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/510510/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-036>

* CONFIRM:

<http://support.apple.com/kb/HT4077>

* APPLE: APPLE-SA-2010-03-29-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>

* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>

* OVAL: oval:org.mitre.oval:def:6626

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6626>

CVE Reference:

CVE-2010-0062 (cve.mitre.org, nvd.nist.gov)

• 18920 QuickTime heap buffer overflow exists in the handling of H.261 encoded movie files (Remote File Checking)

A heap buffer overflow exists in the handling of H.261 encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by performing additional validation of H.261 encoded movie files.

The issue has been fixed in version 7.6.6.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT4077>

* APPLE: APPLE-SA-2010-03-29-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>

* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>

* OVAL: oval:org.mitre.oval:def:7043

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7043>

CVE Reference:

CVE-2010-0514 (cve.mitre.org, nvd.nist.gov)

• 18921 QuickTime memory corruption in the handling of H.264 encoded movie files (Remote File Checking)

A memory corruption in the 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 issue is addressed by performing additional validation of H.264 encoded movie files.

The issue has been fixed in version 7.6.6.

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

References:

- * CONFIRM:
<http://support.apple.com/kb/HT4077>
- * APPLE: APPLE-SA-2010-03-29-1
<http://lists.apple.com/archives/security-announce/2010//Mar/msg00001.html>
- * APPLE: APPLE-SA-2010-03-30-1
<http://lists.apple.com/archives/security-announce/2010//Mar/msg00002.html>
- * OVAL: oval:org.mitre.oval:def:6783
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6783>

CVE Reference:

CVE-2010-0515 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-2739 Microsoft CVSS 2.0 Score = 7.2

Buffer overflow in the CreateDIBPalette function in win32k.sys in Microsoft Windows XP SP3, Server 2003 R2 Enterprise SP2, Vista Business SP1, Windows 7, and Server 2008 SP2 allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.

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

References:

- VUPEN: <http://www.vupen.com/english/advisories/2010/2029>
- MISC: <http://www.ragestorm.net/blogs/?p=255>
- SECUNIA: <http://secunia.com/advisories/40870>
- CONFIRM:
<http://blogs.technet.com/b/msrc/archive/2010/08/10/update-on-the-publicly-disclosed-win32k-sys-eop-vulnerability.aspx>

CVE Reference: [CVE-2010-2739](http://cve.mitre.org/cve/2010/2739)

• CVE-2010-3213 Microsoft CVSS 2.0 Score = 6.8

Cross-site request forgery (CSRF) vulnerability in Microsoft Outlook Web Access (owa/ev.owa) 2007 through SP2 allows remote attackers to hijack the authentication of e-mail users for requests that perform Outlook requests, as demonstrated by setting the auto-forward rule.

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

References:

- XF: <http://xforce.iss.net/xforce/xfdb/60164>
- BID: <http://www.securityfocus.com/bid/41462>
- EXPLOIT-DB: <http://www.exploit-db.com/exploits/14285>
- MISC: <http://sites.google.com/site/tentacoloviola/pwning-corporate-webmails>

CVE Reference: [CVE-2010-3213](http://cve.mitre.org/cve/2010/3213)

• CVE-2010-3004 HP CVSS 2.0 Score = 7.5

Unspecified vulnerability in HP Operations Agent 7.36 and 8.6 on Windows allows remote attackers to execute arbitrary code via unknown vectors. Per:
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02497800> 'A potential security vulnerability has been identified with HP Operations Agent running on Windows.'

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

References:

- SECUNIA: <http://secunia.com/advisories/41277>
- HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02497800>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02497800>

CVE Reference: [CVE-2010-3004](#)

• **CVE-2010-3007 HP CVSS 2.0 Score = 7.2**

Unspecified vulnerability in HP Data Protector Express, and Data Protector Express Single Server Edition (SSE), 3.x before build 56936 and 4.x before build 56906 allows local users to gain privileges or cause a denial of service via unknown vectors.

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

References:

HP: http://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02498535

HP: http://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02498535

CVE Reference: [CVE-2010-3007](#)

• **CVE-2010-3005 HP CVSS 2.0 Score = 6.8**

Unspecified vulnerability in HP Operations Agent 7.36 and 8.6 on Windows allows local users to gain privileges via unknown vectors.

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

References:

SECUNIA: <http://secunia.com/advisories/41277>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02497800>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02497800>

CVE Reference: [CVE-2010-3005](#)

• **CVE-2010-1809 Apple CVSS 2.0 Score = 10.0**

The Accessibility component in Apple iOS before 4.1 on the iPhone and iPod touch does not perform the expected VoiceOver announcement associated with the location services icon, which has unspecified impact and attack vectors.

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

References:

CONFIRM: <http://support.apple.com/kb/HT4334>

APPLE: <http://lists.apple.com/archives/security-announce/2010//Sep/msg00002.html>

CVE Reference: [CVE-2010-1809](#)

• **CVE-2010-2521 Linux CVSS 2.0 Score = 10.0**

Multiple buffer overflows in fs/nfsd/nfs4xdr.c in the XDR implementation in the NFS server in the Linux kernel before 2.6.34-rc6 allow remote attackers to cause a denial of service (panic) or possibly execute arbitrary code via a crafted NFSv4 compound WRITE request, related to the read_buf and nfsd4_decode_compound functions.

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

References:

REDHAT: <https://rhn.redhat.com/errata/RHSA-2010-0606.html>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=612028

BID: <http://www.securityfocus.com/bid/42249>

MLIST: <http://www.openwall.com/lists/oss-security/2010/07/09/2>

MLIST: <http://www.openwall.com/lists/oss-security/2010/07/07/1>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/testing/v2.6.34/ChangeLog-2.6.34-rc6>

SECTRACK: <http://securitytracker.com/id?1024286>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=2bc3c1179c781b359d4f2f3439cb3df72afc17fc>

CVE Reference: [CVE-2010-2521](#)

• **CVE-2010-2495 Linux CVSS 2.0 Score = 10.0**

The pppol2tp_xmit function in drivers/net/pppol2tp.c in the L2TP implementation in the Linux kernel before 2.6.34 does not properly validate certain values associated with an interface, which allows attackers to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via vectors related to a routing change.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=607054

MLIST: <http://www.openwall.com/lists/oss-security/2010/07/06/11>

MLIST: <http://www.openwall.com/lists/oss-security/2010/07/04/3>

MLIST: <http://www.openwall.com/lists/oss-security/2010/07/04/2>

MLIST: <http://www.openwall.com/lists/oss-security/2010/06/23/3>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.34>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=3feec9095d12e311b7d4eb7fe7e5dfa75d4a72a5>

CVE Reference: [CVE-2010-2495](#)

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