

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

What's next, your car? Nigerian scam among top ten online cons. New remote logoff function for better security. Social media service bombarded with spam.

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

• Cars: the next hacking frontier?

That nice, new computerized car you just bought could be hackable.

Of course, your car is probably not a high-priority target for most malicious hackers. But security experts tell CNET that car hacking is starting to move from the realm of the theoretical to reality, thanks to new wireless technologies and evermore dependence on computers to make cars safer, more energy efficient, and modern.

"Now there are computerized systems and they have control over critical components of cars like gas, brakes, etc.," said Adriel Desautels, chief technology officer and president of NetraGard, which does vulnerability assessments and penetration testing on all kinds of systems. "There is a premature reliance on technology." Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20015184-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Nigerian scam tops list of decade's online cons

We've all received e-mails from deposed Nigerian princes asking for help in getting lots of money out of their country. But that's just one of several scams that made Panda Security's list of the most frequent online cons of a decade.

As 2010 starts to wind down, the security vendor on Thursday unveiled its rankings of the most widespread Internet scams from the past 10 years. Though the cons themselves may vary, the pattern is typically the same, according to Panda. Cybercriminals initially contact their victims through e-mail or a social network, asking them to respond back by e-mail, phone, fax, or some other means. The crooks will then try to gain the trust of anyone who swallows the bait, eventually finding some excuse to request money.

The seven scams ranked by Panda included the Nigerian con at the top followed by a variety of other favorites. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20015433-83.html?part=rss&subj=news&tag=2547-1_3-0-20

• Facebook adds new remote log-out security feature

The new Facebook security feature lets people see what devices are logged into their account and to remotely log them off.

(Credit: Facebook)

Facebook on Thursday announced a new security feature that will allow users to see if they are logged into their accounts on a different computer and to remotely log out if so. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20015482-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Spammers inundate Apple's new social media service Ping

Spammers reacted quickly to Apple's new social media service Ping, with reports of users being bombarded with junk messages.

Ping became available with Wednesday's iTunes 10 update, which also includes fixes for 13 flaws. The new service allows users to create a profile and "follow" friends or artists and share status updates, photos, album reviews and information about music purchases.

Sensing the popularity of the new service, criminals already have pounced. The problem for users is that Apple appears to not have implemented any spam or URL filtering protection in Ping, Chet Wisniewski, senior security adviser at Sophos, told SCMagazineUS.com on Friday. SC Magazine

Full Story :

http://www.scmagazineus.com/spammers-inundate-apples-new-social-media-service-ping/article/178211/?utm_source=

New Vulnerabilities Tested in SecureScout

• 14595 Adobe Acrobat / Reader Integer overflow in CoolType.dll Vulnerability (Remote File Checking)

Integer overflow in CoolType.dll in Adobe Reader 8.2.3 and 9.3.3, and Acrobat 9.3.3, allows remote attackers to execute arbitrary code via a TrueType font with a large maxCompositePoints value in a Maximum Profile (maxp) table.

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

References:

* MISC:

<http://securityevaluators.com/files/papers/CrashAnalysis.pdf>

* MISC:

<http://www.zdnet.co.uk/news/security-threats/2010/08/04/adobe-confirms-pdf-security-hole-in-reader-40089737/>

* OVAL: oval:org.mitre.oval:def:11693

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11693>

* SECUNIA: 40766

<http://secunia.com/advisories/40766>

* VUPEN: VUPEN/ADV-2010-2123

<http://www.vupen.com/english/advisories/2010/2123>

* BID: 42203

<http://www.securityfocus.com/bid/42203>

CVE Reference:

CVE-2010-2862 (cve.mitre.org, nvd.nist.gov)

• 18903 OpenSSL "Record of death" Vulnerability

In TLS connections, certain incorrectly formatted records can cause an OpenSSL client or server to crash due to a read attempt at NULL.

Affected versions depend on the C compiler used with OpenSSL:

- If 'short' is a 16-bit integer, this issue applies only to OpenSSL 0.9.8m.
- Otherwise, this issue applies to OpenSSL 0.9.8f through 0.9.8m.

The vulnerability affects the OpenSSL branch 0.9.8 from 0.9.8f to 0.9.8n (not included).

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

References:

- * CONFIRM:
http://www.openssl.org/news/secadv_20100324.txt
- * CONFIRM:
http://aix.software.ibm.com/aix/efixes/security/openssl_advisory.asc
- * FEDORA: FEDORA-2010-5744
<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038587.html>
- * MANDRIVA: MDVSA-2010:076
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:076>
- * SECTRACK: 1023748
<http://www.securitytracker.com/id?1023748>
- * SECUNIA: 39932
<http://secunia.com/advisories/39932>
- * VUPEN: ADV-2010-0710
<http://www.vupen.com/english/advisories/2010/0710>
- * VUPEN: ADV-2010-0839
<http://www.vupen.com/english/advisories/2010/0839>
- * VUPEN: ADV-2010-0933
<http://www.vupen.com/english/advisories/2010/0933>
- * VUPEN: ADV-2010-1216
<http://www.vupen.com/english/advisories/2010/1216>

CVE Reference:

CVE-2010-0740 (cve.mitre.org, nvd.nist.gov)

• 18904 OpenSSL Invalid ASN1 module definition for CMS Vulnerability

CMS structures containing OriginatorInfo are mishandled this can write to invalid memory addresses or free up memory twice (CVE-2010-0742).

This bug is only present in the CMS code: the older PKCS#7 code is not affected.

CMS is only present in OpenSSL 0.9.8h and later where it is disabled by default and 1.0.0 where it is enabled by default.

Users of OpenSSL CMS code should update to 0.9.8o or 1.0.0a which contains a patch to correct this issue.

The vulnerability has been addressed in OpenSSL version 0.9.8o and 1.0.0a.

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

References:

- * CONFIRM:
<http://cvs.openssl.org/chngview?cn=19693>
- * CONFIRM:
http://cvs.openssl.org/filediff?f=openssl/crypto/cms/cms_asn1.c&v1=1.8&v2=1.8.6.1
- * CONFIRM:
<http://rt.openssl.org/Ticket/Display.html?id=2211&user=guest&pass=guest>
- * CONFIRM:
http://www.openssl.org/news/secadv_20100601.txt
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=598738
- * BID: 40502
<http://www.securityfocus.com/bid/40502>

* SECUNIA: 40000
<http://secunia.com/advisories/40000>
* SECUNIA: 40024
<http://secunia.com/advisories/40024>
* VUPEN: ADV-2010-1313
<http://www.vupen.com/english/advisories/2010/1313>

CVE Reference:

CVE-2010-0742 (cve.mitre.org, nvd.nist.gov)

• 18905 OpenSSL Invalid Return value check in pkey_rsa_verifyrecover Vulnerability

When verification recovery fails for RSA keys an uninitialised buffer with an undefined length is returned instead of an error code (CVE-2010-1633).

This bug is only present in OpenSSL 1.0.0 and only affects applications that call the function `EVP_PKEY_verify_recover()`. As this function is not present in previous versions of OpenSSL and not used by OpenSSL internal code very few applications should be affected. The OpenSSL utility application "pkeyutil" does use this function.

The vulnerability has been addressed in OpenSSL version 1.0.0a.

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

References:

* CONFIRM:
<http://cvs.openssl.org/chngview?cn=19693>
* CONFIRM:
http://cvs.openssl.org/filediff?f=openssl/crypto/rsa/rsa_pmeth.c&v1=1.34&v2=1.34.2.1
* CONFIRM:
http://www.openssl.org/news/secadv_20100601.txt
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=598732
* BID: 40503
<http://www.securityfocus.com/bid/40503>
* SECUNIA: 40024
<http://secunia.com/advisories/40024>
* VUPEN: ADV-2010-1313
<http://www.vupen.com/english/advisories/2010/1313>

CVE Reference:

CVE-2010-1633 (cve.mitre.org, nvd.nist.gov)

• 18906 PHP error in the session extension "safe_mode" and "open_basedir" bypass Vulnerability

session.c in the session extension in PHP before 5.2.13, and 5.3.1, does not properly interpret ; (semicolon) characters in the argument to the session_save_path function, which allows context-dependent attackers to bypass open_basedir and safe_mode restrictions via an argument that contains multiple ; characters in conjunction with a .. (dot dot).

The issue has been fixed in PHP version 5.2.13 and 5.3.1.

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

References:

* SREASONRES: 20100211 PHP 5.2.12/5.3.1 session.save_path safe_mode and open_basedir bypass
http://securityreason.com/achievement_securityalert/82
* CONFIRM:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/session/session.c?r1=293036&r2=294272
* CONFIRM:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/session/session.c?view=log
* CONFIRM:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/session/session.c?r1=293036&r2=294272
* CONFIRM:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/session/session.c?view=log
* CONFIRM:
<http://www.php.net/ChangeLog-5.php>
* CONFIRM:
http://www.php.net/releases/5_2_13.php

* SECTRACK: 1023661
<http://securitytracker.com/id?1023661>
* SECUNIA: 38708
<http://secunia.com/advisories/38708>
* SREASON: 7008
<http://securityreason.com/securityalert/7008>
* VUPEN: ADV-2010-0479
<http://www.vupen.com/english/advisories/2010/0479>

CVE Reference:

CVE-2010-1130 (cve.mitre.org, nvd.nist.gov)

• 18907 PHP validation error in the "tempnam()" function "safe_mode" bypass Vulnerability

The safe_mode implementation in PHP before 5.2.13 does not properly handle directory pathnames that lack a trailing / (slash) character, which allows context-dependent attackers to bypass intended access restrictions via vectors related to use of the tempnam function.

The issue has been fixed in PHP version 5.2.13.

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

References:

* CONFIRM:
<http://www.php.net/ChangeLog-5.php>
* CONFIRM:
http://www.php.net/releases/5_2_13.php
* CONFIRM:
<http://support.apple.com/kb/HT4312>
* APPLE: APPLE-SA-2010-08-24-1
<http://lists.apple.com/archives/security-announce/2010/Aug/msg00003.html>
* HP: HPSBMA02554
http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02286083
* BID: 38431
<http://www.securityfocus.com/bid/38431>
* SECTRACK: 1023661
<http://securitytracker.com/id?1023661>
* SECUNIA: 38708
<http://secunia.com/advisories/38708>
* SECUNIA: 40551
<http://secunia.com/advisories/40551>
* VUPEN: ADV-2010-0479
<http://www.vupen.com/english/advisories/2010/0479>
* VUPEN: ADV-2010-1796
<http://www.vupen.com/english/advisories/2010/1796>

CVE Reference:

CVE-2010-1129 (cve.mitre.org, nvd.nist.gov)

• 18908 PHP Linear Congruential Generator information disclosure Vulnerability

The Linear Congruential Generator (LCG) in PHP before 5.2.13 does not provide the expected entropy, which makes it easier for context-dependent attackers to guess values that were intended to be unpredictable, as demonstrated by session cookies generated by using the uniqid function.

The issue has been fixed in PHP version 5.2.13.

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

References:

* CONFIRM:
<http://www.php.net/ChangeLog-5.php>
* CONFIRM:
http://www.php.net/releases/5_2_13.php
* BID: 38430
<http://www.securityfocus.com/bid/38430>
* SECUNIA: 38708
<http://secunia.com/advisories/38708>
* VUPEN: ADV-2010-0479

<http://www.vupen.com/english/advisories/2010/0479>

CVE Reference:

CVE-2010-1128 (cve.mitre.org, nvd.nist.gov)

• 18909 PHP var_export function information disclosure Vulnerability

The var_export function in PHP 5.2 before 5.2.14 and 5.3 before 5.3.3 flushes the output buffer to the user when certain fatal errors occur, even if display_errors is off, which allows remote attackers to obtain sensitive information by causing the application to exceed limits for memory, execution time, or recursion.

The issue has been fixed in PHP versions 5.2.14 and 5.3.3.

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

References:

* MLIST: [oss-security] 20100713 CVE request, php var_export

<http://www.openwall.com/lists/oss-security/2010/07/13/1>

* MLIST: [oss-security] 20100716 Re: CVE request, php var_export

<http://www.openwall.com/lists/oss-security/2010/07/16/3>

* CONFIRM:

http://svn.php.net/viewvc/php/php-src/trunk/ext/standard/tests/general_functions/var_export_error2.phpt?view=log&pathrev=24342

* CONFIRM:

<http://www.php.net/archive/2010.php#id2010-07-22-1>

* CONFIRM:

<http://www.php.net/archive/2010.php#id2010-07-22-2>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=617673

* CONFIRM:

<http://support.apple.com/kb/HT4312>

* APPLE: APPLE-SA-2010-08-24-1

<http://lists.apple.com/archives/security-announce/2010//Aug/msg00003.html>

CVE Reference:

CVE-2010-2531 (cve.mitre.org, nvd.nist.gov)

• 18910 PHP SplObjectStorage unserializer Use-after-free Vulnerability

Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.

The issue has been fixed in PHP versions 5.2.14 and 5.3.3.

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

References:

* MISC:

<http://pastebin.com/mXGidCsd>

* MISC:

<http://twitter.com/i0n1c/statuses/16373156076>

* MISC:

<http://twitter.com/i0n1c/statuses/16447867829>

* MISC:

https://bugzilla.redhat.com/show_bug.cgi?id=605641

* CONFIRM:

<http://support.apple.com/kb/HT4312>

* APPLE: APPLE-SA-2010-08-24-1

<http://lists.apple.com/archives/security-announce/2010//Aug/msg00003.html>

* DEBIAN: DSA-2089

<http://www.debian.org/security/2010/dsa-2089>

* BID: 40948

<http://www.securityfocus.com/bid/40948>

* SECUNIA: 40860

<http://secunia.com/advisories/40860>

* XF: php-splobjectstorage-code-execution(59610)

<http://xforce.iss.net/xfdb/59610>

CVE Reference:

CVE-2010-2225 (cve.mitre.org, nvd.nist.gov)

• **18911 PHP php_mysqlnd_auth_write function Stack-based buffer overflow Vulnerability**

Stack-based buffer overflow in the php_mysqlnd_auth_write function in the Mysqlnd extension in PHP 5.3 through 5.3.2 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long (1) username or (2) database name argument to the (a) mysql_connect or (b) mysqli_connect function.

The issue has been fixed in PHP versions 5.3.3.

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

References:

* MISC:

http://php-security.org/2010/05/31/mops-2010-059-php-php_mysqlnd_auth_write-stack-buffer-overflow-vulnerability/index.

* 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-2010-3064 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2010-3138 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in the Indeo filter (iac25_32.ax) in Microsoft Windows, as used in BS.Player, Media Player Classic, and possibly other products, allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse iacenc.dll that is located in the same folder as an AVI, .mka, .ra, or .ram file. NOTE: some of these details are obtained from third party information. Per: <http://cwe.mitre.org/data/definitions/426.html> 'CWE-426 - 'Untrusted Search Path Vulnerability'

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

References:

MISC: <http://www.zeroscience.mk/en/vulnerabilities/ZSL-2010-4956.php>

SECUNIA: <http://secunia.com/advisories/41114>

CVE Reference: [CVE-2010-3138](http://cve.mitre.org/cve/2010/3138)

• **CVE-2010-3139 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in Microsoft Windows Progman Group Converter (grpconv.exe) allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse imm.dll that is located in the same folder as a .grp file.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/2200>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/14758>

SECUNIA: <http://secunia.com/advisories/41136>

CVE Reference: [CVE-2010-3139](http://cve.mitre.org/cve/2010/3139)

• **CVE-2010-3140 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in Microsoft Windows Internet Communication Settings on Windows XP SP3 allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse schannel.dll that is located in the same folder as an ISP file. Per: <http://cwe.mitre.org/data/definitions/426.html> 'CWE-426 - 'Untrusted Search Path Vulnerability'

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

References:

EXPLOIT-DB: <http://www.exploit-db.com/exploits/14780>

CVE Reference: [CVE-2010-3140](#)

• **CVE-2010-3141 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in Microsoft Power Point 2010 allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse pptimconv.dll that is located in the same folder as a .odp, .pot, .potm, .potx, .ppa, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .pwz, .sldm, or .sldx file.

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

References:

EXPLOIT-DB: <http://www.exploit-db.com/exploits/14723/>

CVE Reference: [CVE-2010-3141](#)

• **CVE-2010-3142 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in Microsoft Office PowerPoint 2007 allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse rpawinet.dll that is located in the same folder as a .odp, .pothtml, .potm, .potx, .ppa, .ppam, .pps, .ppt, .ppthtml, .pptm, .pptxml, .pwz, .sldm, .sldx, and .thmx file. Per: <http://cwe.mitre.org/data/definitions/426.html> 'CWE-426 - 'Untrusted Search Path Vulnerability'

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

References:

EXPLOIT-DB: <http://www.exploit-db.com/exploits/14782/>

CVE Reference: [CVE-2010-3142](#)

• **CVE-2010-3143 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in Microsoft Windows Contacts allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse wab32res.dll that is located in the same folder as a .contact, .group, .p7c, .vcf, or .wab file.

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

References:

EXPLOIT-DB: <http://www.exploit-db.com/exploits/14778/>

CVE Reference: [CVE-2010-3143](#)

• **CVE-2010-3144 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in Microsoft Internet Connection Signup Wizard allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse smmscrpt.dll that is located in the same folder as an ISP file.

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

References:

EXPLOIT-DB: <http://www.exploit-db.com/exploits/14754/>

CVE Reference: [CVE-2010-3144](#)

• **CVE-2010-3145 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in the Microsoft Vista BitLocker Drive Encryption API allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse fveapi.dll that is located in the same folder as a .wbcat file.

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

References:

EXPLOIT-DB: <http://www.exploit-db.com/exploits/14751/>

CVE Reference: [CVE-2010-3145](#)

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