

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

[Request Tracker for Windows \(WinRT\) by SecureScout v3.0.16 alpha](#) - Download Free WinRT v3.0.16 alpha installer by filling our download form. Size: 33MB

Download Here:

http://www.netvigilance.com/productdownloads?productname=winrt_setup_3_0_16

This Week in Review

Security spendings up. Companies need to find out how to view social networking. Survey shows companies are struggling with how to protect their data. Social gaming and age.

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

• Gartner finds IT security spending up eight percent

Despite many organizations facing flat-lining overall budgets due to the ailing economy, security software spending does not appear to be following suffering along, according to new figures from Gartner.

The research firm revealed Monday that it expects the worldwide software security market to total \$14.5 billion this year, up eight percent from last year. The trend will continue next year, when Gartner anticipates the market will see a 13-percent gain in revenue to \$16.3 billion.

The largest growth areas likely will be software-as-a-service and appliance offerings, according to Gartner. Small-and-medium-size businesses are expected to provide the greatest percentage jump in spending, as SMB owners "...are in catch-up mode compared with large companies," Ruggero Contu, a principal research analyst at Gartner, said in a statement. SC Magazine

Full Story :

<http://www.scmagazineus.com/Gartner-finds-IT-security-spending-up-eight-percent/article/149366/>

• Employers grappling with social network use

Social networking is on the rise, both on and off the job, leaving companies uncertain how to monitor their use by employees, reports new survey.

More than 50 percent of companies questioned said they have no policy to address the use of social networking by employees outside the workplace, according to a survey released Wednesday by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association.

Typically, companies shy away from restricting an employee's actions off the job. But businesses are concerned about employees who use social networking and reveal private details or post inappropriate pictures that could embarrass the company. Cnet Security

Full Story :

http://news.cnet.com/8301-10797_3-10360849-235.html?part=rss&subj=news&tag=2547-1_3-0-20

• Survey: Most organizations struggling to secure data

Hampered with issues such as lack of CEO support and budgetary resources, organizations are struggling to secure sensitive data and the majority have experienced a breach, according to a survey released Wednesday by the Ponemon Institute and sponsored by data security company Imperva.

The survey of 517 U.S. and multinational IT security practitioners who are involved in their company's efforts to comply with the Payment Card Industry (PCI) Data Security Standard (DSS), found that 71 percent of respondents believe their organization does not view data security as a strategic initiative across the enterprise. Larry Ponemon, chairman and founder of the Ponemon Institute said in a recent podcast about the survey that he finds that statistic "very disturbing," because failing to treat data protection as a strategic business initiative could ultimately lead to loss of customer confidence and trust. SC Magazine

Full Story :

<http://www.scmagazineus.com/Survey-Most-organizations-struggling-to-secure-data/article/149506/>

• How age impacts social-gaming monetization

New data released by Gambit, a micro-transaction platform provider, illustrates the complexity of both customer targeting and analyzing micro-transaction buying patterns. The major takeaway: older players seem like a good target market until you dig in to find out that they don't spend a whole lot.

But, it takes a minute to understand the data, as Gambit's Susan Su points out in a blog post on how age impacts social-gaming monetization. While it would appear that older users are a good target market thanks to their high revenue-per-user statistic, they are actually pretty meaningless in terms of revenue.

. Cnet Security

Full Story :

http://news.cnet.com/8301-13846_3-10361353-62.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 18522 Wireshark AFS dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the AFS dissector in Wireshark 0.9.2 through 1.2.0 allows remote attackers to cause a denial of service (crash) via unknown vectors.

The vulnerability is reported in versions 0.9.2 to 1.0.8, and 1.2.0.

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

References:

* MLIST: [oss-security] Re: Wireshark - wnpa-sec-2009-05.html &wnpa-sec-2009-06.html -- CVE confirmation and CVE Request

<http://www.openwall.com/lists/oss-security/2009/09/18/2>

* MLIST: [oss-security] Wireshark - wnpa-sec-2009-05.html &wnpa-sec-2009-06.html -- CVE confirmation and CVE Request

<http://www.openwall.com/lists/oss-security/2009/09/17/15>

* MISC:

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=3564

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-04.html>

* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-05.html>
* MANDRIVA: MDVSA-2009:194
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:194>
* BID: 35748
<http://www.securityfocus.com/bid/35748>
* SECUNIA: 35884
<http://secunia.com/advisories/35884>
* VUPEN: ADV-2009-1970
<http://www.vupen.com/english/advisories/2009/1970>

CVE Reference:

CVE-2009-2562 (cve.mitre.org, nvd.nist.gov)

• 18523 Wireshark Infiniband dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the Infiniband dissector in Wireshark when running on unspecified platforms, allows remote attackers to cause a denial of service (crash) via unknown vectors.

The vulnerability is reported in versions 0.9.2 to 1.0.8, and 1.2.0.

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

References:

* MLIST: [oss-security] Wireshark - wnpa-sec-2009-05.html & wnpa-sec-2009-06.html -- CVE confirmation and CVE Request
<http://www.openwall.com/lists/oss-security/2009/09/17/15>
* MLIST: [oss-security] Re: Wireshark - wnpa-sec-2009-05.html & wnpa-sec-2009-06.html -- CVE confirmation and CVE Request
<http://www.openwall.com/lists/oss-security/2009/09/18/2>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-04.html>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-05.html>
* MANDRIVA: MDVSA-2009:194
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:194>
* BID: 35748
<http://www.securityfocus.com/bid/35748>
* SECUNIA: 35884
<http://secunia.com/advisories/35884>
* VUPEN: ADV-2009-1970
<http://www.vupen.com/english/advisories/2009/1970>

CVE Reference:

CVE-2009-2563 (cve.mitre.org, nvd.nist.gov)

• 18524 Wireshark OpcUa dissector Denial of Service (resource consumption) Vulnerability (Remote File Checking)

Unspecified vulnerability in the OpcUa (OPC UA) dissector in Wireshark 0.99.6 through 1.0.8 and 1.2.0 through 1.2.1 allows remote attackers to cause a denial of service (memory and CPU consumption) via malformed OPCUA Service CallRequest packets.

The vulnerability is reported in versions 0.99.6 to 1.0.8, and 1.2.0 to 1.2.1.

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

References:

* MISC:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=3986
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-05.html>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-06.html>
* BID: 36408
<http://www.securityfocus.com/bid/36408>
* SECUNIA: 36754
<http://secunia.com/advisories/36754>

CVE Reference:

CVE-2009-3241 ([cve.mitre.org](https://cve.mitre.org/cve/2009/3241), [nvd.nist.gov](https://nvd.nist.gov/vuln/detail/CVE-2009-3241))

• **18525 Wireshark GSM A RR dissector Denial of Service Vulnerability (Remote File Checking)**

Unspecified vulnerability in packet.c in the GSM A RR dissector in Wireshark 1.2.0 and 1.2.1 allows remote attackers to cause a denial of service (application crash) via unknown vectors related to "an uninitialized dissector handle," which triggers an assertion failure.

The vulnerability is reported in versions 1.2.0 to 1.2.1.

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

References:

- * MISC:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=3893
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-06.html>
- * BID: 36408
<http://www.securityfocus.com/bid/36408>
- * SECUNIA: 36754
<http://secunia.com/advisories/36754>

CVE Reference:

CVE-2009-3242 ([cve.mitre.org](https://cve.mitre.org/cve/2009/3242), [nvd.nist.gov](https://nvd.nist.gov/vuln/detail/CVE-2009-3242))

• **18526 Wireshark TLS dissector Denial of Service Vulnerability (Remote File Checking)**

Unspecified vulnerability in the TLS dissector in Wireshark 1.2.0 and 1.2.1, when running on Windows, allows remote attackers to cause a denial of service (application crash) via unknown vectors related to TLS 1.2 conversations.

The vulnerability is reported in versions 1.2.0 to 1.2.1.

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

References:

- * MISC:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4008
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-06.html>
- * BID: 36408
<http://www.securityfocus.com/bid/36408>
- * SECUNIA: 36754
<http://secunia.com/advisories/36754>

CVE Reference:

CVE-2009-3243 ([cve.mitre.org](https://cve.mitre.org/cve/2009/3243), [nvd.nist.gov](https://nvd.nist.gov/vuln/detail/CVE-2009-3243))

• **18527 PHP php_openssl_apply_verification_policy spoofing certificate Vulnerability**

The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.

The issue has been fixed in PHP versions 5.2.11.

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

References:

- * CONFIRM:
<http://www.php.net/ChangeLog-5.php#5.2.11>
- * CONFIRM:
http://www.php.net/releases/5_2_11.php
- * OSVDB: 58185
<http://www.osvdb.org/58185>
- * SECUNIA: 36791
<http://secunia.com/advisories/36791>
- * XF: php-certificate-unspecified(53334)
<http://xforce.iss.net/xforce/xfdb/53334>

CVE Reference:

CVE-2009-3291 (cve.mitre.org, nvd.nist.gov)

• **18528 PHP missing sanity checks around exif processing Vulnerability**

Unspecified vulnerability in PHP before 5.2.11 has unknown impact and attack vectors related to "missing sanity checks around exif processing."

The issue has been fixed in PHP versions 5.2.11.

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

References:

- * CONFIRM:
<http://www.php.net/ChangeLog-5.php#5.2.11>
- * CONFIRM:
http://www.php.net/releases/5_2_11.php
- * OSVDB: 58186
<http://www.osvdb.org/58186>
- * SECUNIA: 36791
<http://secunia.com/advisories/36791>

CVE Reference:

CVE-2009-3292 (cve.mitre.org, nvd.nist.gov)

• **18529 PHP sanity check for the color index Vulnerability**

Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."

The issue has been fixed in PHP versions 5.2.11.

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

References:

- * CONFIRM:
<http://www.php.net/ChangeLog-5.php#5.2.11>
- * CONFIRM:
http://www.php.net/releases/5_2_11.php
- * OSVDB: 58187
<http://www.osvdb.org/58187>
- * SECUNIA: 36791
<http://secunia.com/advisories/36791>

CVE Reference:

CVE-2009-3293 (cve.mitre.org, nvd.nist.gov)

• **18530 PHP popen crashes with an invalid mode Vulnerability**

The popen API function in TSRM/tsrm_win32.c in PHP before 5.2.11, when running on certain Windows operating systems, allows context-dependent attackers to cause a denial of service (crash) via a crafted (1) "e" or (2) "er" string in the second argument (aka mode), possibly related to the _fdopen function in the Microsoft C runtime library. NOTE: this might not cross privilege boundaries except in rare cases in which the mode argument is accessible to an attacker outside of an application that uses the popen function.

The issue has been fixed in PHP versions 5.2.11.

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

References:

- * MLIST: [oss-security] 20090920 Re: CVE Request -- PHP 5 - 5.2.11
<http://www.openwall.com/lists/oss-security/2009/09/20/1>
- * CONFIRM:
<http://bugs.php.net/bug.php?id=44683>
- * CONFIRM:
<http://svn.php.net/viewvc?view=revision&revision=287779>
- * CONFIRM:
<http://www.php.net/ChangeLog-5.php#5.2.11>
- * CONFIRM:
http://www.php.net/releases/5_2_11.php
- * OSVDB: 58188

<http://www.osvdb.org/58188>

CVE Reference:

CVE-2009-3294 (cve.mitre.org, nvd.nist.gov)

• 18531 Mozilla Firefox - Chrome privilege escalation with FeedWriter vulnerability (Remote File Checking)

Mozilla security researcher moz_bug_r_a4 reported that the BrowserFeedWriter could be leveraged to run JavaScript code from web content with elevated privileges. Using this vulnerability, an attacker could construct an object containing malicious JavaScript and cause the FeedWriter to process the object, running the malicious code with chrome privileges.

The issue has been fixed in Firefox 3.0.14 and 3.5.3.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-51.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=454363
- * REDHAT: RHSA-2009:1430
<http://www.redhat.com/support/errata/RHSA-2009-1430.html>
- * SECTRAK: 1022873
<http://www.securitytracker.com/id?1022873>
- * SECUNIA: 36671
<http://secunia.com/advisories/36671>

CVE Reference:

CVE-2009-3079 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-3275 Microsoft CVSS 2.0 Score = 5.0

Blocks/Common/Src/Configuration/Manageability/Adm/AdmContentBuilder.cs in Microsoft patterns & practices Enterprise Library (aka EntLib) allows context-dependent attackers to cause a denial of service (CPU consumption) via an input string composed of many \ (backslash) characters followed by a " (double quote), related to a certain regular expression, aka a "ReDoS" vulnerability.

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

References:

- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/506419/100/0/threaded>
- MISC: http://www.checkmarx.com/Upload/Documents/PDF/Checkmarx_OWASP_IL_2009_ReDoS.pdf

CVE Reference: [CVE-2009-3275](http://cve.mitre.org/cve/2009/3275)

• CVE-2009-2680 HP CVSS 2.0 Score = 8.5

Unspecified vulnerability in the Remote Management Interface (RMI) for MSL Tape Libraries and 1/8 G2 Tape Autoloaders in HP StorageWorks 1/8 G2 Tape Autoloader firmware 2.30 and earlier, MSL2024 Tape Library firmware 4.20 and earlier, MSL4048 Tape Library firmware 6.50 and earlier, and MSL8096 Tape Library firmware 8.90 and earlier allows remote attackers to cause a denial of service via unknown vectors.

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

References:

- HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01868405>
- HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01868405>
- XF: <http://xforce.iss.net/xforce/xfdb/53237>
- VUPEN: <http://www.vupen.com/english/advisories/2009/2662>

BID: <http://www.securityfocus.com/bid/36388>

OSVDB: <http://www.osvdb.org/58131>

SECTrack: <http://securitytracker.com/id?1022905>

SECUNIA: <http://secunia.com/advisories/36764>

CVE Reference: [CVE-2009-2680](#)

• **CVE-2009-2682 HP CVSS 2.0 Score = 7.2**

Unspecified vulnerability in Role-Based Access Control (RBAC) in HP HP-UX B.11.23 and B.11.31 allows local users to bypass intended access restrictions via unknown vectors.

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

References:

BID: <http://www.securityfocus.com/bid/36476>

HP: <http://marc.info/?l=bugtraq&m=125364434020838&w=2>

HP: <http://marc.info/?l=bugtraq&m=125364434020838&w=2>

CVE Reference: [CVE-2009-2682](#)

• **CVE-2009-2744 IBM CVSS 2.0 Score = 7.8**

Unspecified vulnerability in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.27 allows remote attackers to cause a denial of service via unknown vectors, related to "an error in fixpacks 6.1.0.23 and 6.1.0.25."

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

References:

MISC: <http://www-01.ibm.com/support/docview.wss?uid=swg27007951>

XF: <http://xforce.iss.net/xforce/xfdb/53344>

CVE Reference: [CVE-2009-2744](#)

• **CVE-2009-3291 PHP CVSS 2.0 Score = 7.5**

The `php_openssl_apply_verification_policy` function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.

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

References:

CONFIRM: http://www.php.net/releases/5_2_11.php

CONFIRM: <http://www.php.net/ChangeLog-5.php#5.2.11>

XF: <http://xforce.iss.net/xforce/xfdb/53334>

OSVDB: <http://www.osvdb.org/58185>

SECUNIA: <http://secunia.com/advisories/36791>

CVE Reference: [CVE-2009-3291](#)

• **CVE-2009-3292 PHP CVSS 2.0 Score = 7.5**

Unspecified vulnerability in PHP before 5.2.11 has unknown impact and attack vectors related to "missing sanity checks around exif processing."

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

References:

CONFIRM: http://www.php.net/releases/5_2_11.php

CONFIRM: <http://www.php.net/ChangeLog-5.php#5.2.11>

OSVDB: <http://www.osvdb.org/58186>

SECUNIA: <http://secunia.com/advisories/36791>

CVE Reference: [CVE-2009-3292](#)

• **CVE-2009-3293 PHP CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."

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

References:

CONFIRM: <http://www.php.net/ChangeLog-5.php#5.2.11>

CONFIRM: http://www.php.net/releases/5_2_11.php

OSVDB: <http://www.osvdb.org/58187>

SECUNIA: <http://secunia.com/advisories/36791>

CVE Reference: [CVE-2009-3293](#)

• **CVE-2009-2817 Apple CVSS 2.0 Score = 9.3**

Buffer overflow in Apple iTunes before 9.0.1 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted .pls file.

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

References:

BID: <http://www.securityfocus.com/bid/36478>

CONFIRM: <http://support.apple.com/kb/HT3884>

APPLE: <http://lists.apple.com/archives/security-announce/2009/Sep/msg00006.html>

CVE Reference: [CVE-2009-2817](#)

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