

## 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

Predictions for the year to come. Not all is less secure when going Cloud. China uses IE flaw. Google open about attack - most companies aren't.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netvigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • Opinion: IT's 5 big security mistakes

Computerworld - Happy New Year, folks. As usual, the turn of the calendar has brought no shortage of articles predicting the future. That's all well and good, but it's a good idea to also take stock of where we are before we chart our course forward, so we can truly improve things for the future.

You see, one of my pet peeves with our industry is how abysmal we tend to be at learning from our mistakes. Rather than blithely charging forward only to repeat those mistakes, let's study them and learn from them a bit first.

With that, here are a few things (in no particular order) where we are making some really big mistakes. These are, in my view, some of the real fundamental causes of the biggest problems we're dealing with today -- and into the future, no doubt. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9144300/Opinion IT s 5 big security mistakes?source=rss\\_security](http://www.computerworld.com/s/article/9144300/Opinion_IT_s_5_big_security_mistakes?source=rss_security)

## • Clearing The Cloud 3: Some Security What-ifs

CSO - In the first in his series of "Clearing the Cloud" columns, security expert Ariel Silverstone explored the dangers of jumping too soon into cloud computing. In the second article, he defined relevant risks that we must consider when implementing cloud computing and promised to show us some solutions. In this article, he continues his vision on how to manage and secure cloud-computing solutions.

In the sections that follow I will put forward some ideas on how to resolve issues defined in my two previous articles. I will also attempt to show some of the security-related benefits we can garner from the use of cloud computing, especially those that we could not, or could not easily, do before.

The approach Computerworld

Full Story :

[http://www.computerworld.com/s/article/9144338/Clearing\\_The\\_Cloud\\_3\\_Some\\_Security\\_What\\_ifs?source=rss\\_secu](http://www.computerworld.com/s/article/9144338/Clearing_The_Cloud_3_Some_Security_What_ifs?source=rss_secu)

## • Microsoft discloses zero-day IE flaw used in China attacks

The organized and well-resourced cybercriminals who compromised systems at Google, Adobe and more than 30 other large companies used a previously unknown, zero-day Internet Explorer exploit as part of their arsenal to install data-stealing malware on target machines, researchers at McAfee revealed Thursday.

"As with most targeted attacks, the intruders gained access to an organization by sending a tailored attack to one or a few targeted individuals," George Kurtz, McAfee's CTO, said in a blog post. "We suspect these individuals were targeted because they likely had access to valuable intellectual property. These attacks will look like they come from a trusted source, leading the target to fall for the trap and clicking a link or file. That's when the exploitation takes place, using the vulnerability in Microsoft's Internet Explorer." SC Magazine

Full Story :

[http://www.scmagazineus.com/microsoft-discloses-zero-day-ie-flaw-used-in-china-attacks/article/161418/?utm\\_sour](http://www.scmagazineus.com/microsoft-discloses-zero-day-ie-flaw-used-in-china-attacks/article/161418/?utm_sour)

## • Behind the China attacks on Google (FAQ)

Computer attacks on corporations happen all the time, but most companies don't publicize them. They fear damage to their reputation and they don't want to jeopardize the investigation or reveal any information that could be used in future attacks.

Google shocked the security community on Tuesday by disclosing that it and other companies had been hit by attacks that originated in China, with some targeting Gmail users who were human rights activists. As a result, the search giant said it would stop censoring its Web results in China and could end up exiting that market altogether.

Google hasn't released many details on the attacks or named any of the other companies, and sources seem to have only bits and pieces of information. Here's what CNET knows at this time. Cnet Security

Full Story :

[http://news.cnet.com/8301-27080\\_3-10434721-245.html](http://news.cnet.com/8301-27080_3-10434721-245.html)

## New Vulnerabilities Tested in SecureScout

### • 18672 Microtype Express Compressed Fonts Integer Flaw in the LZCOMP Decompressor Vulnerability (MS10-001/972270) (Remote File Checking)

A remote code execution vulnerability exists in the way that the Microsoft Windows Embedded OpenType (EOT) Font Engine decompresses specially crafted EOT fonts. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

#### References:

\* MS: MS10-001

<http://www.microsoft.com/technet/security/Bulletin/MS10-001.mspx>

\* BID: 37671

<http://www.securityfocus.com/bid/37671>

\* VUPEN: VUPEN/ADV-2010-0095

<http://www.vupen.com/english/advisories/2010/0095>

#### CVE Reference:

CVE-2010-0018 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18673 PHP 'session.save\_path()' Arbitrary Code Execution Vulnerability

PHP before 5.2.12 does not properly handle session data, which allows an attacker to execute arbitrary code related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save\_path directive.

The issue has been fixed in PHP version 5.2.12.

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\\_12.php](http://www.php.net/releases/5_2_12.php)
- \* BID: 37390  
<http://www.securityfocus.com/bid/37390>
- \* SECUNIA: 37821  
<http://secunia.com/advisories/37821>
- \* VUPEN: ADV-2009-3593  
<http://www.vupen.com/english/advisories/2009/3593>

#### CVE Reference:

CVE-2009-4143 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18674 PHP 'htmlspecialchars()' Malformed Multibyte Character Cross Site Scripting Vulnerability

The htmlspecialchars function in PHP before 5.2.12 does not properly handle (1) overlong UTF-8 sequences, (2) invalid Shift\_JIS sequences, and (3) invalid EUC-JP sequences, which allows remote attackers to conduct cross-site scripting (XSS) attacks by placing a crafted byte sequence before a special character.

The issue has been fixed in PHP version 5.2.12.

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

#### References:

- \* CONFIRM:  
<http://bugs.php.net/bug.php?id=49785>
- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php>
- \* CONFIRM:  
[http://www.php.net/releases/5\\_2\\_12.php](http://www.php.net/releases/5_2_12.php)
- \* BID: 37389  
<http://www.securityfocus.com/bid/37389>
- \* SECTRACK: 1023372  
<http://securitytracker.com/id?1023372>
- \* SECUNIA: 37821  
<http://secunia.com/advisories/37821>
- \* VUPEN: ADV-2009-3593  
<http://www.vupen.com/english/advisories/2009/3593>

#### CVE Reference:

CVE-2009-4142 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18675 GD Graphics Library '\_gdGetColors' Remote Buffer Overflow Vulnerability

The \_gdGetColors function in gd\_gd.c in PHP 5.2.11 and 5.3.x before 5.3.1, and the GD Graphics Library 2.x, does not properly verify a certain colorsTotal structure member, which might allow remote attackers to conduct buffer overflow or buffer over-read attacks via a crafted GD file, a different vulnerability than CVE-2009-3293. NOTE: some of these details are obtained from third party information.

The issue has been fixed in PHP version 5.2.12, and 5.3.1.

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

#### References:

\* MLIST: [oss-security] 20091015 Re: CVE Request -- PHP 5 - 5.2.11  
<http://marc.info/?l=oss-security&m=125562113503923&w=2>  
\* MLIST: [oss-security] 20091120 Re: CVE request: php 5.3.1 update  
<http://www.openwall.com/lists/oss-security/2009/11/20/5>  
\* CONFIRM:  
<http://svn.php.net/viewvc?view=revision&revision=289557>  
\* MANDRIVA: MDVSA-2009:285  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:285>  
\* BID: 36712  
<http://www.securityfocus.com/bid/36712>  
\* SECUNIA: 37069  
<http://secunia.com/advisories/37069>  
\* SECUNIA: 37080  
<http://secunia.com/advisories/37080>  
\* VUPEN: ADV-2009-2929  
<http://www.vupen.com/english/advisories/2009/2929>  
\* VUPEN: ADV-2009-2930  
<http://www.vupen.com/english/advisories/2009/2930>

#### CVE Reference:

CVE-2009-3546 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18676 Apache Tomcat Information disclosure Vulnerability (CVE-2002-2009)

Apache Tomcat is a freely available, open source application server maintained by the Apache Foundation.

Apache Tomcat 4.0.1 allows remote attackers to obtain the web root path via HTTP requests for JSP files preceded by (1) +/, (2) >/, (3) </, and (4) %20/, which leaks the pathname in an error message.

The issue affects Apache Tomcat versions:  
4.0.0-4.0.2

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

#### References:

\* BUGTRAQ: 20020419 Tomcat 4.1 real path disclosure  
<http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-04/0286.html>  
\* BUGTRAQ: 20010419 Re: Tomcat 4.1 real path disclosure  
<http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-04/0297.html>  
\* CONFIRM:  
<http://tomcat.apache.org/security-4.html>  
\* BID: 4557  
<http://www.securityfocus.com/bid/4557>  
\* XF: tomcat-jsp-path-disclosure(42915)  
<http://xforce.iss.net/xforce/xfdb/42915>

#### CVE Reference:

CVE-2002-2009 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18677 Apache Tomcat Information disclosure Vulnerability (CVE-2001-0917)

Apache Tomcat is a freely available, open source application server maintained by the Apache Foundation.

Tomcat 4.0.1 allows remote attackers to reveal physical path information by requesting a long URL with a .JSP extension.

The issue affects Apache Tomcat versions:  
4.0.0-4.0.2

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

#### References:

\* BUGTRAQ: 20011122 Hi  
<http://marc.theaimsgroup.com/?l=bugtraq&m=100654722925155&w=2>  
\* CONFIRM:  
<http://marc.theaimsgroup.com/?l=tomcat-dev&m=100658457507305&w=2>  
\* XF: tomcat-reveal-install-path(7599)  
<http://xforce.iss.net/xforce/xfdb/7599>

#### CVE Reference:

CVE-2001-0917 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • **18679 Apache Tomcat Installation path disclosure Vulnerability (CVE-2005-4703)**

Apache Tomcat is a freely available, open source application server maintained by the Apache Foundation.

Apache Tomcat when running on Windows, allows remote attackers to obtain sensitive information via a request for a file that contains an MS-DOS device name such as lpt9, which leaks the pathname in an error message.

The issue affects Apache Tomcat versions:

4.0.0-4.0.3

4.1.0-4.1.3

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

#### References:

\* MISC:

[http://osvdb.org/ref/20/20033-tomcat-dos-path\\_disclosure.txt](http://osvdb.org/ref/20/20033-tomcat-dos-path_disclosure.txt)

\* CONFIRM:

<http://tomcat.apache.org/security-4.html>

\* BID: 28484

<http://www.securityfocus.com/bid/28484>

\* OSVDB: 20033

<http://www.osvdb.org/20033>

\* XF: tomcat-msdos-path-disclosure(42914)

<http://xforce.iss.net/xforce/xfdb/42914>

#### CVE Reference:

CVE-2005-4703 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • **18680 Apache Tomcat Installation path disclosure Vulnerability (CVE-2002-2008)**

Apache Tomcat is a freely available, open source application server maintained by the Apache Foundation.

Apache Tomcat for Windows allows remote attackers to obtain the web root path via an HTTP request for a resource that does not exist, such as lpt9, which leaks the information in an error message.

The issue affects Apache Tomcat versions:

4.0.0-4.0.3

4.1.0-4.1.3

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

#### References:

\* BUGTRAQ: 20020619 KPMG-2002024: Apache Tomcat Path Disclosure

<http://archives.neohapsis.com/archives/bugtraq/2002-06/0225.html>

\* CONFIRM:

<http://tomcat.apache.org/security-4.html>

\* BID: 5054

<http://www.securityfocus.com/bid/5054>

\* XF: tomcat-lpt9-path-disclosure(9394)

[http://www.iss.net/security\\_center/static/9394.php](http://www.iss.net/security_center/static/9394.php)

#### CVE Reference:

CVE-2002-2008 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • **18681 Apache Tomcat Denial of service Vulnerability (CVE-2002-1895)**

Apache Tomcat is a freely available, open source application server maintained by the Apache Foundation.

The servlet engine in Jakarta Apache Tomcat 3.3 and 4.0.4, when using IIS and the ajp1.3 connector, allows remote attackers to cause a denial of service (crash) via a large number of HTTP GET requests for an MS-DOS device such as AUX, LPT1, CON, or PRN.

The issue affects Apache Tomcat versions:

3.3.x

4.0.0-4.0.4

4.1.0-4.1.9

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

## References:

- \* VULNWATCH: 20021011 Apache Tomcat 3.x and 4.0.x: Remote denial-of-service vulnerability  
<http://archives.neohapsis.com/archives/vulnwatch/2002-q4/0020.html>
- \* CONFIRM:  
<http://tomcat.apache.org/security-4.html>
- \* XF: tomcat-get-device-dos(10348)  
[http://www.iss.net/security\\_center/static/10348.php](http://www.iss.net/security_center/static/10348.php)

## CVE Reference:

CVE-2002-1895 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 18682 Apache Tomcat Denial of service Vulnerability (CVE-2005-0808)

Apache Tomcat is a freely available, open source application server maintained by the Apache Foundation.

Tomcat 3.x can be remotely caused to crash or shutdown by a connection sending the right sequence of bytes to the AJP12 protocol port (TCP 8007 by default). Tomcat 3.x users are advised to ensure that this port is adequately firewalled to ensure it is not accessible to remote attackers. There are no plans to issue an update to Tomcat 3.x for this issue.

The issue affects Apache Tomcat versions:

3.x

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

## References:

- \* CONFIRM:  
<http://www.kb.cert.org/vuls/id/JGEI-6A2LEF>
- \* CONFIRM:  
[http://www.hitachi-support.com/security\\_e/vuls\\_e/HS05-006\\_e/index-e.html](http://www.hitachi-support.com/security_e/vuls_e/HS05-006_e/index-e.html)
- \* CERT-VN: VU#204710  
<http://www.kb.cert.org/vuls/id/204710>
- \* BID: 12795  
<http://www.securityfocus.com/bid/12795>
- \* XF: tomcat-manager-ajp12-dos(19681)  
<http://xforce.iss.net/xforce/xfdb/19681>

## CVE Reference:

CVE-2005-0808 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2010-0018 Microsoft CVSS 2.0 Score = 9.3

Integer overflow in the Embedded OpenType (EOT) Font Engine in Microsoft Windows 2000 SP4; Windows XP SP2 and SP3; Windows Server 2003 SP2; Windows Vista Gold, SP1, and SP2; Windows Server 2008 Gold, SP2, and R2; and Windows 7 allows remote attackers to execute arbitrary code via compressed data that represents a crafted EOT font, aka "Microtype Express Compressed Fonts Integer Flaw in the LZCOMP Decompressor Vulnerability." Per: <http://www.microsoft.com/technet/security/Bulletin/MS10-001.mspx> This security update is rated Critical for Microsoft Windows 2000, and is rated Low for Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. For more information, see the subsection, Affected and Non-Affected Software, in this section.

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

## References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-001.mspx>

## CVE Reference: [CVE-2010-0018](http://cve.mitre.org)

### • CVE-2010-0278 Microsoft CVSS 2.0 Score = 4.3

A certain ActiveX control in msgsc.14.0.8089.726.dll in Microsoft Windows Live Messenger 2009 build 14.0.8089.726 on Windows Vista and Windows 7 allows remote attackers to cause a denial of service (msnmsgr.exe crash) by calling the ViewProfile method with a crafted argument during an MSN Messenger session.

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

## References:

BID: <http://www.securityfocus.com/bid/37680>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/508811/100/0/threaded>

**CVE Reference:** [CVE-2010-0278](#)

### • **CVE-2010-0079 Oracle CVSS 2.0 Score = 10.0**

Multiple vulnerabilities in the JRockit component in BEA Product Suite R27.6.5 using JRE/JDK 1.4.2, 5, and 6 allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors. NOTE: this CVE identifier overlaps CVE-2009-3867, CVE-2009-3868, CVE-2009-3869, CVE-2009-3871, CVE-2009-3872, CVE-2009-3873, CVE-2009-3874, CVE-2009-3875, CVE-2009-3876, and CVE-2009-3877.

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

## References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA10-012A.html>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>

**CVE Reference:** [CVE-2010-0079](#)

### • **CVE-2010-0071 Oracle CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the Listener component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

## References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA10-012A.html>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>

**CVE Reference:** [CVE-2010-0071](#)

### • **CVE-2010-0072 Oracle CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.3 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

## References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA10-012A.html>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>

**CVE Reference:** [CVE-2010-0072](#)

### • **CVE-2009-3415 Oracle CVSS 2.0 Score = 9.0**

Unspecified vulnerability in the Oracle OLAP component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.3 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.

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

## References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA10-012A.html>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>

**CVE Reference:** [CVE-2009-3415](#)

### • **CVE-2010-0077 Oracle CVSS 2.0 Score = 6.4**

Unspecified vulnerability in the CRM Technical Foundation (mobile) component in Oracle E-Business Suite 11.5.10.2, 12.0.6, and 12.1.2 allows remote attackers to affect confidentiality and integrity via unknown vectors.

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

## References:

CERT: <http://www.us-cert.gov/cas/techalerts/TA10-012A.html>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>

**CVE Reference:** [CVE-2010-0077](#)

• **CVE-2010-0076 Oracle CVSS 2.0 Score = 6.0**

Unspecified vulnerability in the Application Express Application Builder component in Oracle Database 3.2.1.00.10 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.

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

**References:**

CERT: <http://www.us-cert.gov/cas/techalerts/TA10-012A.html>

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>

**CVE Reference:** [CVE-2010-0076](#)

**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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)