

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

Large 2008 data breach finally settled. Malware hit hard in 09. Encrypted USB data not so secure. Social networking application provider sued

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

• Heartland to pay up to \$60M to Visa over breach

IDG News Service - Heartland Payment Systems will pay up to \$60 million to issuers of Visa credit and debit cards for losses they incurred from a 2008 data breach at the large payment processor.

The settlement between Heartland and Visa, announced today, will offer card issuers "an immediate recovery with respect to losses they may have incurred from the Heartland intrusion," Ellen Richey, Visa's chief enterprise risk officer, said in a statement.

Heartland disclosed the breach a year ago. The U.S. Department of Justice has charged Albert Gonzalez and several other accomplices with the data breach, and Heartland was one of several companies they broke into using SQL injection attacks. Gonzalez and his associates stole more than 130 million credit card numbers from Heartland, prosecutors alleged. Computerworld

Full Story :

http://www.computerworld.com/s/article/9143480/Heartland_to_pay_up_to_60M_to_Visa_over_breach?source=rss_s

• Panda finds 2009 a record-breaking malware year

Cybercriminals pumped out more malware in 2009 than they did in nearly 20 years, according to anti-virus vendor Panda Security. During 2009, PandaLabs, the anti-malware lab of Panda Security, identified 25 million new malware samples, according to Panda Security's Annual Malware Report, released Tuesday. Before 2009, PandaLabs had identified a total of 15 million pieces of malware in 19 years.

Cybercriminals have developed tools to automate the process of replicating malware, allowing them to quickly create several thousand variants of the same malware file, Sean-Paul Correll, threat researcher at PandaLabs, told SCMagazineUS.com on Tuesday. In some cases, they also sell these services to others.

"Cybercriminals have figured out that they can saturate anti-virus labs by creating millions of samples," Correll said. "By doing that they can slow down the response times and their infection ratio would be more successful." SC Magazine

Full Story :

http://www.scmagazineus.com/panda-finds-2009-a-record-breaking-malware-year/article/160687/?utm_source=feedb

• Flaw could allow attacker to decrypt protected USB drives

Several flash drive manufacturers recently issued warnings about a flaw which could allow an attacker to access encrypted data on a supposedly secure USB drive.

Secure flash drives utilize 256-bit AES hardware-based encryption to protect sensitive information. The vulnerability, which affects certain secure Kingston, SanDisk and Verbatim flash drives, is present in the mechanism used to verify an individual's password.

"A skilled person with the proper tools and physical access to the drives may be able to gain unauthorized access to data contained on [certain] Kingston Secure USB drives," Kingston said in an advisory on its website. SC Magazine

Full Story :

http://www.scmagazineus.com/flaw-could-allow-attacker-to-decrypt-protected-usb-drives/article/160772/?utm_source

• RockYou sued over data breach

(Credit: RockYou)

An Indiana man filed a lawsuit against RockYou this week alleging that the provider of social-networking apps failed to secure its network and protect customer data, enabling a hacker to grab passwords of 32 million users earlier this month.

The suit seeking class action status was filed Monday in U.S. District Court in San Francisco by lawyers for Alan Claridge, of Evansville, Ind., who registered with RockYou in August 2008 to use a photo-sharing application. RockYou is a publisher and developer of online apps and services like "SuperWall" on Facebook and "Slideshow" on MySpace. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10423042-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 18662 Apache Tomcat Information Disclosure Vulnerability (CVE-2005-4836)

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

The deprecated HTTP/1.1 connector does not reject request URIs containing null bytes when used with contexts that are configured with allowLinking="true". Failure to reject the null byte enables an attacker to obtain the source for any JSP page in these contexts. Users of Tomcat 4.1.x are advised to use the default, supported Coyote HTTP/1.1 connector which does not exhibit this issue. There are no plans to issue an update to Tomcat 4.1.x for this issue.

The issue has been identified in Apache Tomcat 4.1.15 and above. The issue is not intended to be fixed in the Apache Tomcat branch 4.1.

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

References:

* CONFIRM:

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

* BID: 28483

<http://www.securityfocus.com/bid/28483>

CVE Reference:

CVE-2005-4836 (cve.mitre.org, nvd.nist.gov)

• 18663 Apache Tomcat Information Disclosure Vulnerability (CVE-2005-3164)

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

If a client specifies a Content-Length but disconnects before sending any of the request body, the deprecated AJP connector processes the request using the request body of the previous request. Users are advised to use the default, supported Coyote AJP connector which does not exhibit this issue.

The issue affects the following Apache Tomcat versions:

4.0.1-4.0.6,
4.1.0-4.1.36

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

References:

* CONFIRM:

http://www.hitachi-support.com/security_e/vuls_e/HS05-019_e/01-e.html

* CONFIRM:

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

* CONFIRM:

<http://support.apple.com/kb/HT2163>

* APPLE: APPLE-SA-2008-06-30

<http://lists.apple.com/archives/security-announce/2008/Jun/msg00002.html>

* SUNALERT: 239312

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-239312-1>

* JVN: JVN#79314822

<http://jvn.jp/jp/JVN%2379314822/index.html>

* BID: 15003

<http://www.securityfocus.com/bid/15003>

* VUPEN: ADV-2008-1981

<http://www.frsirt.com/english/advisories/2008/1981/references>

* VUPEN: ADV-2008-1979

<http://www.frsirt.com/english/advisories/2008/1979/references>

* SECUNIA: 17019

<http://secunia.com/advisories/17019>

* SECUNIA: 30802

<http://secunia.com/advisories/30802>

* SECUNIA: 30908

<http://secunia.com/advisories/30908>

* SECUNIA: 30899

<http://secunia.com/advisories/30899>

CVE Reference:

CVE-2005-3164 (cve.mitre.org, nvd.nist.gov)

• 18664 Apache Tomcat Cross-site scripting Vulnerability (CVE-2007-3383)

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

When reporting error messages, the SendMailServlet (part of the examples web application) did not escape user provided data before including it in the output. This enabled a XSS attack. This Servlet now filters the data before use. This issue may be mitigated by undeploying the examples web application. Note that it is recommended that the examples web application is not installed on a production system.

The issue affects the following Apache Tomcat versions:

4.0.0-4.0.6,
4.1.0-4.1.36

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

References:

* BUGTRAQ: 20070721 CVE-2007-3383: XSS in Tomcat send mail example

<http://www.securityfocus.com/archive/1/archive/1/474413/100/0/threaded>

* FULLDISC: 20070721 CVE-2007-3383: XSS in Tomcat send mail example

<http://seclists.org/fulldisclosure/2007/Jul/0448.html>

* CONFIRM:

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

* CONFIRM:

<http://support.apple.com/kb/HT2163>

* APPLE: APPLE-SA-2008-06-30

<http://lists.apple.com/archives/security-announce/2008/Jun/msg00002.html>

* CERT-VN: VU#862600

<http://www.kb.cert.org/vuls/id/862600>

* BID: 24999

<http://www.securityfocus.com/bid/24999>

* VUPEN: ADV-2007-2618

<http://www.frsirt.com/english/advisories/2007/2618>

* VUPEN: ADV-2008-1981

<http://www.frsirt.com/english/advisories/2008/1981/references>

* OSVDB: 39000

<http://osvdb.org/39000>

* SECUNIA: 30802

<http://secunia.com/advisories/30802>

* SREASON: 2918

<http://securityreason.com/securityalert/2918>

* XF: tomcat-sendmail-example-xss(35536)

<http://xforce.iss.net/xforce/xfdb/35536>

CVE Reference:

CVE-2007-3383 (cve.mitre.org, nvd.nist.gov)

• 18665 Apache Tomcat Cross-site scripting Vulnerability (CVE-2002-1567)

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

The unmodified requested URL is included in the 404 response header. The new lines in this URL appear to the client to be the end of the header section. The remaining part of the URL, including the script elements, is treated as part of the response body and the client executes the script. Tomcat now replaces potentially unsafe characters in the response headers with spaces.

The issue affects the following Apache Tomcat versions:

4.1.0-4.1.28

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

References:

* VULN-DEV: 20020821 Apache Tomcat 4.1 Cross-Site Scripting Vulnerability

<http://archives.neohapsis.com/archives/vuln-dev/2002-q3/0482.html>

* CONFIRM:

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

CVE Reference:

CVE-2002-1567 (cve.mitre.org, nvd.nist.gov)

• 18666 Apache Tomcat Information disclosure Vulnerability (CVE-2002-1394)

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

A specially crafted URL using the invoker servlet in conjunction with the default servlet can enable an attacker to obtain the source of JSP pages or, under special circumstances, a static resource that would otherwise have been protected by a security constraint without the need to be properly authenticated. This is a variation of CVE-2002-1148

The issue affects the following Apache Tomcat versions:

4.0.0-4.0.5,

4.1.0-4.1.12

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

References:

* DEBIAN: DSA-225

<http://www.debian.org/security/2003/dsa-225>

* CONFIRM:

<http://marc.theaimsgroup.com/?l=tomcat-dev&m=103417249325526&w=2>

* CONFIRM:

http://issues.apache.org/bugzilla/show_bug.cgi?id=13365

* REDHAT: RHSA-2003:075
<http://www.redhat.com/support/errata/RHSA-2003-075.html>
* REDHAT: RHSA-2003:082
<http://www.redhat.com/support/errata/RHSA-2003-082.html>
* GENTOO: GLSA-200210-001
<http://marc.theaimsgroup.com/?l=bugtraq&m=103470282514938&w=2>
* BID: 6562
<http://www.securityfocus.com/bid/6562>
* XF: tomcat-invoker-source-code(10376)
<http://xforce.iss.net/xforce/xfdb/10376>

CVE Reference:

CVE-2002-1394 (cve.mitre.org, nvd.nist.gov)

• 18667 Apache Tomcat Cross-site scripting Vulnerability (CVE-2002-0682)

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

A specially crafted URL using the invoker servlet and various internal classes causes Tomcat to throw an exception that includes unescaped information from the malformed request. This allows the XSS attack.

The issue affects the following Apache Tomcat versions:

4.0.0-4.0.5,
4.1.0-4.1.12

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

References:

* BUGTRAQ: 20020710 wp-02-0008: Apache Tomcat Cross Site Scripting
<http://marc.theaimsgroup.com/?l=bugtraq&m=102631703811297&w=2>
* VULNWATCH: 20020710 [VulnWatch] wp-02-0008: Apache Tomcat Cross Site Scripting
<http://archives.neohapsis.com/archives/vulnwatch/2002-q3/0014.html>
* XF: tomcat-servlet-xss(9520)
<http://xforce.iss.net/xforce/xfdb/9520>
* BID: 5193
<http://www.securityfocus.com/bid/5193>
* OSVDB: 4973
<http://www.osvdb.org/4973>

CVE Reference:

CVE-2002-0682 (cve.mitre.org, nvd.nist.gov)

• 18668 Apache Tomcat Information disclosure Vulnerability (CVE-2002-1148)

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

A specially crafted URL using the default servlet can enable an attacker to obtain the source of JSP pages.

The issue affects the following Apache Tomcat versions:

4.0.0-4.0.4,
4.1.0-4.1.11

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

References:

* BUGTRAQ: 20020924 JSP source code exposure in Tomcat 4.x
<http://marc.theaimsgroup.com/?l=bugtraq&m=103288242014253&w=2>
* DEBIAN: DSA-170
<http://www.debian.org/security/2002/dsa-170>
* HP: HPSBUX0212-229
<http://online.securityfocus.com/advisories/4758>
* REDHAT: RHSA-2002:217
<http://www.redhat.com/support/errata/RHSA-2002-217.html>
* REDHAT: RHSA-2002:218
<http://www.redhat.com/support/errata/RHSA-2002-218.html>
* BID: 5786
<http://www.securityfocus.com/bid/5786>
* XF: tomcat-servlet-source-code(10175)
http://www.iss.net/security_center/static/10175.php

CVE Reference:

CVE-2002-1148 (cve.mitre.org, nvd.nist.gov)

• 18669 Apache Tomcat Denial of service Vulnerability (CVE-2002-0935)

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

A malformed HTTP request can cause the request processing thread to become unresponsive. A sequence of such requests will cause all request processing threads, and hence Tomcat as a whole, to become unresponsive.

The issue affects the following Apache Tomcat versions:

4.0.0-4.0.6,
4.1.0-4.1.2

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

References:

* VULNWATCH: 20020620 [VulnWatch] KPMG-2002025: Apache Tomcat Denial of Service
<http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0120.html>

* BUGTRAQ: 20020620 KPMG-2002025: Apache Tomcat Denial of Service
<http://online.securityfocus.com/archive/1/277940>

* XF: tomcat-null-thread-dos(9396)
http://www.iss.net/security_center/static/9396.php

* BID: 5067
<http://www.securityfocus.com/bid/5067>

* OSVDB: 5051
<http://www.osvdb.org/5051>

CVE Reference:

CVE-2002-0935 (cve.mitre.org, nvd.nist.gov)

• 18670 Apache Tomcat Denial of service Vulnerability (CVE-2003-0866)

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

A malformed HTTP request can cause the request processing thread to become unresponsive. A sequence of such requests will cause all request processing threads, and hence Tomcat as a whole, to become unresponsive.

The issue affects the following Apache Tomcat versions:

4.0.0-4.0.6

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

References:

* CONFIRM:
<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=215506>

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

* DEBIAN: DSA-395
<http://www.debian.org/security/2003/dsa-395>

* SUNALERT: 239312
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-239312-1>

* BID: 8824
<http://www.securityfocus.com/bid/8824>

* VUPEN: ADV-2008-1979
<http://www.frsirt.com/english/advisories/2008/1979/references>

* SECUNIA: 30908
<http://secunia.com/advisories/30908>

* SECUNIA: 30899
<http://secunia.com/advisories/30899>

* XF: tomcat-non-http-dos(13429)
<http://xforce.iss.net/xforce/xfdb/13429>

CVE Reference:

CVE-2003-0866 (cve.mitre.org, nvd.nist.gov)

• 18671 Apache Tomcat Information disclosure Vulnerability (CVE-2002-2006)

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

The snoop and trouble shooting servlets installed as part of the examples include output that identifies the Tomcat installation path.

The issue affects the following Apache Tomcat versions:

4.0.0-4.0.6

3.1-3.1.1,

3.2-3.2.4

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

References:

* BUGTRAQ: 20020422 Tomcat real path disclosure (2)

<http://archives.neohapsis.com/archives/bugtraq/2002-04/0311.html>

* CONFIRM:

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

* SUNALERT: 239312

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-239312-1>

* BID: 4575

<http://www.securityfocus.com/bid/4575>

* VUPEN: ADV-2008-1979

<http://www.frsirt.com/english/advisories/2008/1979/references>

* SECUNIA: 30908

<http://secunia.com/advisories/30908>

* SECUNIA: 30899

<http://secunia.com/advisories/30899>

* XF: tomcat-example-class-information(8932)

http://www.iss.net/security_center/static/8932.php

CVE Reference:

CVE-2002-2006 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-4565 Sendmail CVSS 2.0 Score = 7.5

sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/3661>

CONFIRM: <http://www.sendmail.org/releases/8.14.4>

BID: <http://www.securityfocus.com/bid/37543>

SECUNIA: <http://secunia.com/advisories/37998>

CVE Reference: [CVE-2009-4565](http://cve.mitre.org)

• CVE-2010-0220 Mozilla CVSS 2.0 Score = 5.0

The nsObserverList::FillObserverArray function in xpcdm/ds/nsObserverList.cpp in Mozilla Firefox before 3.5.7 allows remote attackers to cause a denial of service (application crash) via a crafted web site that triggers memory consumption and an accompanying Low Memory alert dialog, and also triggers attempted removal of an observer from an empty observers array.

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

References:

CONFIRM: <http://www.mozilla.com/en-US/firefox/3.5.7/releasenotes/>

MISC: <http://isc.sans.org/diary.html?storyid=7897>

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=507114

CONFIRM: <http://hg.mozilla.org/mozilla-central/rev/51396f6c9f20>

CVE Reference: [CVE-2010-0220](#)

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