

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

US and Russia discussing security. Rogue anti virus costly. Adobe looking into alleged exploit. US wants tougher policy.

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

• U.S. and Russian officials talk cyberissues

In a notable policy shift, American and Russian officials have met to discuss cybersecurity issues, such as collaboration among law enforcement bodies and the use of cyberweapons, the New York Times reported in its Saturday editions.

Under the Bush administration, U.S. officials simply "refused to engage" with the Russians on cyberissues, James Lewis, director of technology and public policy at the Center for Strategic International Studies, told SCMagazineUS.com on Monday.

But in mid-November, Gen. Vladislav Sherstyuk, deputy secretary of the Russian Security Council, along with other Russian officials, including the former leader of the Russian equivalent of the National Security Agency, met in Washington with representatives of the National Security Council and the State, Defense and Homeland Security departments, the Times reported on Saturday. SC Magazine

Full Story :

• **FBI: Fraudsters earned \$150 million in rogue AV scams**

For the first time, the FBI has issued a public warning about the threat of rogue anti-virus software, which the agency said has resulted in more than \$150 million in losses to victims.

In an intelligence note posted Friday on the website of the Internet Crime Complaint Center, the FBI said users should be on the lookout for pop-up advertisements masking as legitimate-looking AV software, known as "rogueware" or "scareware."

Rogue anti-virus software typically is purveyed through malicious advertisements, or "malvertisements," on trusted websites. When viewed or clicked, the ads lead users to sites that claim their computer is infected and, to resolve the issue, they should buy an anti-virus product, which turns out to be fake. In other instances, the ads try to install trojans onto the victim's PC. SC Magazine

Full Story :

http://www.scmagazineus.com/fbi-fraudsters-earned-150-million-in-rogue-av-scams/article/159597/?utm_source=feedburner&utm_medium=feed

• **Adobe investigating Reader, Acrobat exploit reports**

Adobe warned of reports of an attack exploiting a hole in Reader and Acrobat on Monday.

"This afternoon, Adobe received reports of a vulnerability in Adobe Reader and Acrobat 9.2 and earlier versions being exploited in the wild," the company said in an advisory on its Security Incident Response Team blog. "We are currently investigating this issue and assessing the risk to our customers. We will provide an update as soon as we have more information."

Three different security vendor partners reported the alleged exploit to the company on Monday afternoon, said Adobe spokeswoman Wiebke Lips. She said she could not provide more details. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10415438-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• **U.S. House to toughen internal cybersecurity policy**

Congressional leaders on Tuesday accepted five new cybersecurity policy recommendations aimed at protecting sensitive information belonging to the U.S. House and securing its IT systems from attack.

The proposed changes were crafted by Daniel Beard, the House's chief administrative officer, who was asked by Speaker Nancy Pelosi and Minority Leader John Boehner to conduct an assessment of the lower chamber's information security policies.

The new guidelines, set to take effect next year, require all House staff and members to undergo an annual cybersecurity training program, according to a letter from Beard to his House colleagues. Employees who travel out of the country will be required to have their wireless devices and laptops screened for malware prior to departing and upon returning. SC Magazine

Full Story :

http://www.scmagazineus.com/us-house-to-toughen-internal-cybersecurity-policy/article/159785/?utm_source=feedburner&utm_medium=feed

New Vulnerabilities Tested in SecureScout

• **18630 Apache Tomcat Cross-site scripting Vulnerability (CVE-2007-2449)**

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

JSPs within the examples web application did not escape user provided data before including it in the output. This enabled a XSS attack. These JSPs now filter 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 Apache Tomcat versions:

6.0.0-6.0.13

5.0.0-5.0.30

5.5.0-5.5.24

4.0.0-4.0.6

4.1.0-4.1.36

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

References:

- * BUGTRAQ: 20070614 [CVE-2007-2449] Apache Tomcat XSS vulnerabilities in the JSP examples
<http://www.securityfocus.com/archive/1/archive/1/471351/100/0/threaded>
- * BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)
<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>
- * BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities
<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>
- * CONFIRM:
<http://tomcat.apache.org/security-6.html>
- * CONFIRM:
<http://tomcat.apache.org/security-4.html>
- * CONFIRM:
<http://tomcat.apache.org/security-5.html>
- * CONFIRM:
<http://support.apple.com/kb/HT2163>
- * CONFIRM:
<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>
- * CONFIRM:
<http://support.ca.com/iri/portal/anonymous/phpsupcontent?contentID=197540>
- * APPLE: APPLE-SA-2008-06-30
<http://lists.apple.com/archives/security-announce/2008/Jun/msg00002.html>
- * FEDORA: FEDORA-2007-3456
<https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00525.html>
- * HP: HPSBUX02262
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>
- * MANDRIVA: MDKSA-2007:241
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:241>
- * REDHAT: RHSA-2007:0569
<http://www.redhat.com/support/errata/RHSA-2007-0569.html>
- * REDHAT: RHSA-2008:0261
<http://www.redhat.com/support/errata/RHSA-2008-0261.html>
- * REDHAT: RHSA-2008:0630
<http://rhn.redhat.com/errata/RHSA-2008-0630.html>
- * SUSE: SUSE-SR:2008:007
<http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00008.html>
- * SUSE: SUSE-SR:2009:004
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>
- * BID: 24476
<http://www.securityfocus.com/bid/24476>
- * VUPEN: ADV-2007-2213
<http://www.frsirt.com/english/advisories/2007/2213>
- * VUPEN: ADV-2007-3386
<http://www.frsirt.com/english/advisories/2007/3386>
- * VUPEN: ADV-2008-1981
<http://www.frsirt.com/english/advisories/2008/1981/references>
- * VUPEN: ADV-2009-0233
<http://www.frsirt.com/english/advisories/2009/0233>
- * SECTRAK: 1018245
<http://www.securitytracker.com/id?1018245>
- * SECUNIA: 26076
<http://secunia.com/advisories/26076>
- * SECUNIA: 27037
<http://secunia.com/advisories/27037>
- * SECUNIA: 27727
<http://secunia.com/advisories/27727>
- * SECUNIA: 29392
<http://secunia.com/advisories/29392>
- * SECUNIA: 30802
<http://secunia.com/advisories/30802>
- * SECUNIA: 31493
<http://secunia.com/advisories/31493>
- * SECUNIA: 33668
<http://secunia.com/advisories/33668>
- * SREASON: 2804
<http://securityreason.com/securityalert/2804>
- * XF: tomcat-example-xss(34869)
<http://xforce.iss.net/xforce/xfdb/34869>

CVE Reference:

• 18631 Apache Tomcat Cross-site scripting Vulnerability (CVE-2007-2450)

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

The Manager and Host Manager web applications did not escape user provided data before including it in the output. This enabled a XSS attack. These applications now filter the data before use. This issue may be mitigated by logging out (closing the browser) of the application once the management tasks have been completed.

The issue affects Apache Tomcat versions:

6.0.0-6.0.13
5.0.0-5.0.30
5.5.0-5.5.24
4.0.0-4.0.6
4.1.0-4.1.36

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

References:

- * BUGTRAQ: 20070614 [CVE-2007-2450]: Apache Tomcat XSS vulnerability in Manager
<http://www.securityfocus.com/archive/1/archive/1/471357/100/0/threaded>
- * BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)
<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>
- * BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities
<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>
- * CONFIRM:
<http://tomcat.apache.org/security-6.html>
- * CONFIRM:
<http://tomcat.apache.org/security-4.html>
- * CONFIRM:
<http://tomcat.apache.org/security-5.html>
- * CONFIRM:
<http://support.apple.com/kb/HT2163>
- * CONFIRM:
<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>
- * CONFIRM:
<http://support.ca.com/iri/portal/anonymous/phpsupcontent?contentID=197540>
- * APPLE: APPLE-SA-2008-06-30
<http://lists.apple.com/archives/security-announce/2008/Jun/msg00002.html>
- * DEBIAN: DSA-1468
<http://www.debian.org/security/2008/dsa-1468>
- * FEDORA: FEDORA-2007-3456
<https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00525.html>
- * HP: HPSBUX02262
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>
- * MANDRIVA: MDKSA-2007:241
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:241>
- * REDHAT: RHSA-2007:0569
<http://www.redhat.com/support/errata/RHSA-2007-0569.html>
- * REDHAT: RHSA-2008:0261
<http://www.redhat.com/support/errata/RHSA-2008-0261.html>
- * SUNALERT: 239312
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-239312-1>
- * SUSE: SUSE-SR:2009:004
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>
- * JVN: JVN#07100457
<http://jvn.jp/jp/JVN%2307100457/index.html>
- * BID: 24475
<http://www.securityfocus.com/bid/24475>
- * VUPEN: ADV-2007-2213
<http://www.frsirt.com/english/advisories/2007/2213>
- * VUPEN: ADV-2007-3386
<http://www.frsirt.com/english/advisories/2007/3386>
- * 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>
- * VUPEN: ADV-2009-0233
<http://www.frsirt.com/english/advisories/2009/0233>

* OSVDB: 36079
<http://www.osvdb.org/36079>
* SECTRACK: 1018245
<http://www.securitytracker.com/id?1018245>
* SECUNIA: 25678
<http://secunia.com/advisories/25678>
* SECUNIA: 26076
<http://secunia.com/advisories/26076>
* SECUNIA: 27037
<http://secunia.com/advisories/27037>
* SECUNIA: 27727
<http://secunia.com/advisories/27727>
* SECUNIA: 28549
<http://secunia.com/advisories/28549>
* SECUNIA: 30802
<http://secunia.com/advisories/30802>
* SECUNIA: 30908
<http://secunia.com/advisories/30908>
* SECUNIA: 30899
<http://secunia.com/advisories/30899>
* SECUNIA: 33668
<http://secunia.com/advisories/33668>
* SREASON: 2813
<http://securityreason.com/securityalert/2813>
* XF: tomcat-hostmanager-xss(34868)
<http://xforce.iss.net/xforce/xfdb/34868>

CVE Reference:

CVE-2007-2450 (cve.mitre.org, nvd.nist.gov)

• 18632 Apache Tomcat Session hi-jacking Vulnerability (CVE-2007-3382)

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

Tomcat incorrectly treated a single quote character (') in a cookie value as a delimiter. In some circumstances this lead to the leaking of information such as session ID to an attacker.

The issue affects Apache Tomcat versions:

6.0.0-6.0.13
5.0.0-5.0.30
5.5.0-5.5.24
4.1.0-4.1.36
3.3-3.3.2

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

References:

* BUGTRAQ: 20070814 CVE-2007-3382: Handling of cookies containing a ' character
<http://www.securityfocus.com/archive/1/archive/1/476442/100/0/threaded>
* BUGTRAQ: 20070814 Re: CVE-2007-3382: Handling of cookies containing a ' character
<http://www.securityfocus.com/archive/1/archive/1/476466/100/0/threaded>
* BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)
<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>
* BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities
<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>
* CONFIRM:
<http://tomcat.apache.org/security-6.html>
* CONFIRM:
<http://support.apple.com/kb/HT2163>
* CONFIRM:
<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>
* CONFIRM:
<http://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=197540>
* AIXAPAR: IZ55562
<http://www-01.ibm.com/support/docview.wss?uid=swg1IZ55562>
* APPLE: APPLE-SA-2008-06-30
<http://lists.apple.com/archives/security-announce/2008/Jun/msg00002.html>
* DEBIAN: DSA-1447
<http://www.debian.org/security/2008/dsa-1447>

* DEBIAN: DSA-1453
<http://www.debian.org/security/2008/dsa-1453>

* FEDORA: FEDORA-2007-3456
<https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00525.html>

* HP: HPSBUX02262
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>

* HP: HPSBTU02276
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01192554>

* MANDRIVA: MDKSA-2007:241
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:241>

* REDHAT: RHSA-2007:0871
<http://www.redhat.com/support/errata/RHSA-2007-0871.html>

* REDHAT: RHSA-2007:0950
<http://www.redhat.com/support/errata/RHSA-2007-0950.html>

* REDHAT: RHSA-2008:0195
<http://www.redhat.com/support/errata/RHSA-2008-0195.html>

* REDHAT: RHSA-2008:0261
<http://www.redhat.com/support/errata/RHSA-2008-0261.html>

* SUSE: SUSE-SR:2008:005
<http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00001.html>

* SUSE: SUSE-SR:2009:004
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>

* CERT-VN: VU#993544
<http://www.kb.cert.org/vuls/id/993544>

* BID: 25316
<http://www.securityfocus.com/bid/25316>

* SECUNIA: 36486
<http://secunia.com/advisories/36486>

* VUPEN: ADV-2007-2902
<http://www.frsirt.com/english/advisories/2007/2902>

* VUPEN: ADV-2007-3386
<http://www.frsirt.com/english/advisories/2007/3386>

* VUPEN: ADV-2007-3527
<http://www.frsirt.com/english/advisories/2007/3527>

* VUPEN: ADV-2008-1981
<http://www.frsirt.com/english/advisories/2008/1981/references>

* VUPEN: ADV-2009-0233
<http://www.frsirt.com/english/advisories/2009/0233>

* SECTRAK: 1018556
<http://securitytracker.com/id?1018556>

* SECUNIA: 26466
<http://secunia.com/advisories/26466>

* SECUNIA: 26898
<http://secunia.com/advisories/26898>

* SECUNIA: 27037
<http://secunia.com/advisories/27037>

* SECUNIA: 27267
<http://secunia.com/advisories/27267>

* SECUNIA: 27727
<http://secunia.com/advisories/27727>

* SECUNIA: 28317
<http://secunia.com/advisories/28317>

* SECUNIA: 28361
<http://secunia.com/advisories/28361>

* SECUNIA: 29242
<http://secunia.com/advisories/29242>

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

* SECUNIA: 33668
<http://secunia.com/advisories/33668>

* XF: tomcat-quotecookie-information-disclosure(36006)
<http://xforce.iss.net/xforce/xfdb/36006>

CVE Reference:

CVE-2007-3382 (cve.mitre.org, nvd.nist.gov)

• 18633 Apache Tomcat Session hi-jacking Vulnerability (CVE-2007-3385)

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

Tomcat incorrectly handled the character sequence \" in a cookie value. In some circumstances this lead to the leaking of information such as session ID to an attacker.

The issue affects Apache Tomcat versions:

6.0.0-6.0.13
5.0.0-5.0.30
5.5.0-5.5.24
4.1.0-4.1.36
3.3-3.3.2

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

References:

- * BUGTRAQ: 20070814 CVE-2007-3385: Handling of \" in cookies
<http://www.securityfocus.com/archive/1/archive/1/476444/100/0/threaded>
- * BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)
<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>
- * BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities
<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>
- * CONFIRM:
<http://tomcat.apache.org/security-6.html>
- * CONFIRM:
<http://support.apple.com/kb/HT2163>
- * CONFIRM:
<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>
- * CONFIRM:
<http://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=197540>
- * AIXAPAR: IZ55562
<http://www-01.ibm.com/support/docview.wss?uid=swg1IZ55562>
- * APPLE: APPLE-SA-2008-06-30
<http://lists.apple.com/archives/security-announce/2008/Jun/msg00002.html>
- * DEBIAN: DSA-1447
<http://www.debian.org/security/2008/dsa-1447>
- * DEBIAN: DSA-1453
<http://www.debian.org/security/2008/dsa-1453>
- * FEDORA: FEDORA-2007-3456
<https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00525.html>
- * HP: HPSBUX02262
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>
- * HP: HPSBTU02276
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01192554>
- * MANDRIVA: MDKSA-2007:241
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:241>
- * REDHAT: RHSA-2007:0871
<http://www.redhat.com/support/errata/RHSA-2007-0871.html>
- * REDHAT: RHSA-2007:0950
<http://www.redhat.com/support/errata/RHSA-2007-0950.html>
- * REDHAT: RHSA-2008:0195
<http://www.redhat.com/support/errata/RHSA-2008-0195.html>
- * REDHAT: RHSA-2008:0261
<http://www.redhat.com/support/errata/RHSA-2008-0261.html>
- * SUSE: SUSE-SR:2008:005
<http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00001.html>
- * SUSE: SUSE-SR:2009:004
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>
- * CERT-VN: VU#993544
<http://www.kb.cert.org/vuls/id/993544>
- * BID: 25316
<http://www.securityfocus.com/bid/25316>
- * SECUNIA: 36486
<http://secunia.com/advisories/36486>
- * VUPEN: ADV-2007-2902
<http://www.frsirt.com/english/advisories/2007/2902>
- * VUPEN: ADV-2007-3386
<http://www.frsirt.com/english/advisories/2007/3386>
- * VUPEN: ADV-2007-3527
<http://www.frsirt.com/english/advisories/2007/3527>
- * VUPEN: ADV-2008-1981
<http://www.frsirt.com/english/advisories/2008/1981/references>

* VUPEN: ADV-2009-0233
<http://www.frsirt.com/english/advisories/2009/0233>
* SECTRAK: 1018557
<http://securitytracker.com/id?1018557>
* SECUNIA: 26466
<http://secunia.com/advisories/26466>
* SECUNIA: 26898
<http://secunia.com/advisories/26898>
* SECUNIA: 27037
<http://secunia.com/advisories/27037>
* SECUNIA: 27267
<http://secunia.com/advisories/27267>
* SECUNIA: 27727
<http://secunia.com/advisories/27727>
* SECUNIA: 28317
<http://secunia.com/advisories/28317>
* SECUNIA: 28361
<http://secunia.com/advisories/28361>
* SECUNIA: 29242
<http://secunia.com/advisories/29242>
* SECUNIA: 30802
<http://secunia.com/advisories/30802>
* SECUNIA: 33668
<http://secunia.com/advisories/33668>
* SREASON: 3011
<http://securityreason.com/securityalert/3011>
* XF: tomcat-slashcookie-information-disclosure(35999)
<http://xforce.iss.net/xforce/xfdb/35999>

CVE Reference:

CVE-2007-3385 (cve.mitre.org, nvd.nist.gov)

• 18634 Apache Tomcat Cross-site scripting Vulnerability (CVE-2007-1355)

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

The JSP and Servlet included in the sample application within the Tomcat documentation webapp did not escape user provided data before including it in the output. This enabled a XSS attack. These pages have been simplified not to use any user provided data in the output.

The issue affects Apache Tomcat versions:

6.0.0-6.0.10
5.0.0-5.0.30
5.5.0-5.5.23
4.0.1-4.0.6
4.1.0-4.1.36

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

References:

* BUGTRAQ: 20070519 [CVE-2007-1355] Tomcat documentation XSS vulnerabilities
<http://www.securityfocus.com/archive/1/archive/1/469067/100/0/threaded>
* BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)
<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>
* BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities
<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>
* CONFIRM:
<http://tomcat.apache.org/security-4.html>
* CONFIRM:
<http://tomcat.apache.org/security-5.html>
* CONFIRM:
<http://tomcat.apache.org/security-6.html>
* CONFIRM:
<http://support.apple.com/kb/HT2163>
* CONFIRM:
<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>
* CONFIRM:
<http://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=197540>
* APPLE: APPLE-SA-2008-06-30

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

* FEDORA: FEDORA-2007-3456

<https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00525.html>

* HP: HPSBUX02262

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>

* REDHAT: RHSA-2008:0261

<http://www.redhat.com/support/errata/RHSA-2008-0261.html>

* REDHAT: RHSA-2008:0630

<http://rhn.redhat.com/errata/RHSA-2008-0630.html>

* SUNALERT: 239312

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

* BID: 24058

<http://www.securityfocus.com/bid/24058>

* OVAL: oval:org.mitre.oval:def:6111

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6111>

* VUPEN: ADV-2007-3386

<http://www.frsirt.com/english/advisories/2007/3386>

* 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>

* VUPEN: ADV-2009-0233

<http://www.frsirt.com/english/advisories/2009/0233>

* SECUNIA: 27037

<http://secunia.com/advisories/27037>

* SECUNIA: 27727

<http://secunia.com/advisories/27727>

* SECUNIA: 30802

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

* SECUNIA: 30908

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

* SECUNIA: 30899

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

* SECUNIA: 31493

<http://secunia.com/advisories/31493>

* SECUNIA: 33668

<http://secunia.com/advisories/33668>

* SREASON: 2722

<http://securityreason.com/securityalert/2722>

* XF: tomcat-hello-xss(34377)

<http://xforce.iss.net/xforce/xfdb/34377>

CVE Reference:

CVE-2007-1355 (cve.mitre.org, nvd.nist.gov)

• 18635 Apache Tomcat Information Disclosure Vulnerability (CVE-2005-2090)

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

Requests with multiple content-length headers should be rejected as invalid. When multiple components (firewalls, caches, proxies and Tomcat) process a sequence of requests where one or more requests contain multiple content-length headers and several components do not reject the request and make different decisions as to which content-length header to use an attacker can poison a web-cache, perform an XSS attack and obtain sensitive information from requests other than their own. Tomcat now returns 400 for requests with multiple content-length headers.

The issue affects Apache Tomcat versions:

6.0.0-6.0.10

5.0.0-5.0.30

5.5.0-5.5.22

4.0.0-4.0.6

4.1.0-4.1.34

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

References:

* BUGTRAQ: 20050606 A new whitepaper by Watchfire - HTTP Request Smuggling

<http://seclists.org/lists/bugtraq/2005/Jun/0025.html>

* BUGTRAQ: 20080108 VMSA-2008-0002 Low severity security update for VirtualCenter and ESX Server 3.0.2,

and ESX 3.0.1

<http://www.securityfocus.com/archive/1/archive/1/485938/100/0/threaded>

* BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)

<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>

* BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities

<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>

* MLIST: [Security-announce] 20080107 VMSA-2008-0002 Low severity security update for VirtualCenter and ESX Server 3.0.2, and ESX 3.0.1

<http://lists.vmware.com/pipermail/security-announce/2008/000003.html>

* MISC:

<http://www.watchfire.com/resources/HTTP-Request-Smuggling.pdf>

* MISC:

<http://www.securiteam.com/securityreviews/5GP0220G0U.html>

* CONFIRM:

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

* CONFIRM:

<http://tomcat.apache.org/security-5.html>

* CONFIRM:

<http://tomcat.apache.org/security-6.html>

* CONFIRM:

<http://docs.info.apple.com/article.html?artnum=306172>

* CONFIRM:

<http://www.fujitsu.com/global/support/software/security/products-f/interstage-200703e.html>

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2007-206.htm>

* CONFIRM:

<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>

* CONFIRM:

<http://support.ca.com/iri/portal/anonymous/phpsupcontent?contentID=197540>

* APPLE: APPLE-SA-2007-07-31

<http://lists.apple.com/archives/security-announce/2007/Jul/msg00004.html>

* HP: HPSBUX02262

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>

* REDHAT: RHSA-2007:0327

<http://www.redhat.com/support/errata/RHSA-2007-0327.html>

* REDHAT: RHSA-2007:0360

<http://www.redhat.com/support/errata/RHSA-2007-0360.html>

* REDHAT: RHSA-2008:0261

<http://www.redhat.com/support/errata/RHSA-2008-0261.html>

* SUNALERT: 239312

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

* SUSE: SUSE-SR:2008:005

<http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00001.html>

* BID: 25159

<http://www.securityfocus.com/bid/25159>

* BID: 13873

<http://www.securityfocus.com/bid/13873>

* VUPEN: ADV-2007-2732

<http://www.frsirt.com/english/advisories/2007/2732>

* VUPEN: ADV-2007-3087

<http://www.frsirt.com/english/advisories/2007/3087>

* VUPEN: ADV-2007-3386

<http://www.frsirt.com/english/advisories/2007/3386>

* VUPEN: ADV-2008-0065

<http://www.frsirt.com/english/advisories/2008/0065>

* VUPEN: ADV-2008-1979

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

* VUPEN: ADV-2009-0233

<http://www.frsirt.com/english/advisories/2009/0233>

* SECTRAK: 1014365

<http://securitytracker.com/id?1014365>

* SECUNIA: 26235

<http://secunia.com/advisories/26235>

* SECUNIA: 26660

<http://secunia.com/advisories/26660>

* SECUNIA: 27037

<http://secunia.com/advisories/27037>

* SECUNIA: 28365

<http://secunia.com/advisories/28365>

* SECUNIA: 29242
<http://secunia.com/advisories/29242>
* SECUNIA: 30908
<http://secunia.com/advisories/30908>
* SECUNIA: 30899
<http://secunia.com/advisories/30899>
* SECUNIA: 33668
<http://secunia.com/advisories/33668>

CVE Reference:

CVE-2005-2090 (cve.mitre.org, nvd.nist.gov)

• 18636 Apache Tomcat Directory traversal Vulnerability (CVE-2007-0450)

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

The fix for this issue was insufficient. A fix was also required in the JK connector module for httpd. See CVE-2007-1860 for further information.

Tomcat permits '\', '%2F' and '%5C' as path delimiters. When Tomcat is used behind a proxy (including, but not limited to, Apache HTTP server with mod_proxy and mod_jk) configured to only proxy some contexts, a HTTP request containing strings like "\.\/" may allow attackers to work around the context restriction of the proxy, and access the non-proxied contexts.

The following Java system properties have been added to Tomcat to provide additional control of the handling of path delimiters in URLs (both options default to false):

* org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH: true|false
* org.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH: true|false

Due to the impossibility to guarantee that all URLs are handled by Tomcat as they are in proxy servers, Tomcat should always be secured as if no proxy restricting context access was used.

The issue affects Apache Tomcat versions:

6.0.0-6.0.9
5.0.0-5.0.30
5.5.0-5.5.21
4.0.0-4.0.6
4.1.0-4.1.34

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

References:

* BUGTRAQ: 20080108 VMSA-2008-0002 Low severity security update for VirtualCenter and ESX Server 3.0.2, and ESX 3.0.1
<http://www.securityfocus.com/archive/1/archive/1/485938/100/0/threaded>
* BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)
<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>
* BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities
<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>
* MLIST: [Security-announce] 20080107 VMSA-2008-0002 Low severity security update for VirtualCenter and ESX Server 3.0.2, and ESX 3.0.1
<http://lists.vmware.com/pipermail/security-announce/2008/000003.html>
* CONFIRM:
<http://tomcat.apache.org/security-4.html>
* CONFIRM:
<http://tomcat.apache.org/security-5.html>
* CONFIRM:
<http://tomcat.apache.org/security-6.html>
* CONFIRM:
<http://docs.info.apple.com/article.html?artnum=306172>
* CONFIRM:
<http://www.fujitsu.com/global/support/software/security/products-f/interstage-200702e.html>
* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2007-206.htm>
* CONFIRM:
<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>
* CONFIRM:
<http://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=197540>

* APPLE: APPLE-SA-2007-07-31
<http://lists.apple.com/archives/security-announce/2007/Jul/msg00004.html>

* GENTOO: GLSA-200705-03
<http://security.gentoo.org/glsa/glsa-200705-03.xml>

* HP: HPSBUX02262
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>

* MANDRIVA: MDKSA-2007:241
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:241>

* REDHAT: RHSA-2007:0327
<http://www.redhat.com/support/errata/RHSA-2007-0327.html>

* REDHAT: RHSA-2007:0360
<http://www.redhat.com/support/errata/RHSA-2007-0360.html>

* REDHAT: RHSA-2008:0261
<http://www.redhat.com/support/errata/RHSA-2008-0261.html>

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

* SUSE: SUSE-SR:2007:005
http://www.novell.com/linux/security/advisories/2007_5_sr.html

* SUSE: SUSE-SR:2007:015
http://www.novell.com/linux/security/advisories/2007_15_sr.html

* BID: 22960
<http://www.securityfocus.com/bid/22960>

* BUGTRAQ: 20070314 SEC Consult SA-20070314-0 :: Apache HTTP Server / Tomcat directory traversal
<http://www.securityfocus.com/archive/1/archive/1/462791/100/0/threaded>

* MISC:
<http://www.sec-consult.com/287.html>

* MISC:
http://www.sec-consult.com/fileadmin/Advisories/20070314-0-apache_tomcat_directory_traversal.txt

* BID: 25159
<http://www.securityfocus.com/bid/25159>

* VUPEN: ADV-2007-0975
<http://www.frsirt.com/english/advisories/2007/0975>

* VUPEN: ADV-2007-2732
<http://www.frsirt.com/english/advisories/2007/2732>

* VUPEN: ADV-2007-3087
<http://www.frsirt.com/english/advisories/2007/3087>

* VUPEN: ADV-2007-3386
<http://www.frsirt.com/english/advisories/2007/3386>

* VUPEN: ADV-2008-0065
<http://www.frsirt.com/english/advisories/2008/0065>

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

* VUPEN: ADV-2009-0233
<http://www.frsirt.com/english/advisories/2009/0233>

* SECUNIA: 24732
<http://secunia.com/advisories/24732>

* SECUNIA: 25106
<http://secunia.com/advisories/25106>

* SECUNIA: 25280
<http://secunia.com/advisories/25280>

* SECUNIA: 26235
<http://secunia.com/advisories/26235>

* SECUNIA: 26660
<http://secunia.com/advisories/26660>

* SECUNIA: 27037
<http://secunia.com/advisories/27037>

* SECUNIA: 28365
<http://secunia.com/advisories/28365>

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

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

* SECUNIA: 33668
<http://secunia.com/advisories/33668>

* SREASON: 2446
<http://securityreason.com/securityalert/2446>

* XF: tomcat-proxy-directory-traversal(32988)
<http://xforce.iss.net/xforce/xfdb/32988>

CVE Reference:

• 18637 Apache Tomcat Cross-site scripting Vulnerability (CVE-2007-1358)

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

Web pages that display the Accept-Language header value sent by the client are susceptible to a cross-site scripting attack if they assume the Accept-Language header value conforms to RFC 2616. Under normal circumstances this would not be possible to exploit, however older versions of Flash player were known to allow carefully crafted malicious Flash files to make requests with such custom headers. Tomcat now ignores invalid values for Accept-Language headers that do not conform to RFC 2616.

The issue affects Apache Tomcat versions:

6.0.0-6.0.5
5.0.0-5.0.30
5.5.0-5.5.20
4.0.0-4.0.6
4.1.0-4.1.34

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

References:

- * BUGTRAQ: 20070618 [CVE-2007-1358] Apache Tomcat XSS vulnerability in Accept-Language header processing
<http://www.securityfocus.com/archive/1/archive/1/471719/100/0/threaded>
- * BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)
<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>
- * BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities
<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>
- * CONFIRM:
<http://tomcat.apache.org/security-4.html>
- * CONFIRM:
<http://docs.info.apple.com/article.html?artnum=306172>
- * CONFIRM:
<http://www.fujitsu.com/global/support/software/security/products-f/interstage-200704e.html>
- * CONFIRM:
<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>
- * CONFIRM:
<http://support.ca.com/iri/portal/anonymous/phpsupcontent?contentID=197540>
- * APPLE: APPLE-SA-2007-07-31
<http://lists.apple.com/archives/security-announce/2007/Jul/msg00004.html>
- * FEDORA: FEDORA-2007-3456
<https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00525.html>
- * HP: HPSBUX02262
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>
- * REDHAT: RHSA-2008:0261
<http://www.redhat.com/support/errata/RHSA-2008-0261.html>
- * REDHAT: RHSA-2008:0630
<http://rhn.redhat.com/errata/RHSA-2008-0630.html>
- * SUNALERT: 239312
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-239312-1>
- * JVN: JVN#16535199
<http://jvn.jp/jp/JVN%2316535199/index.html>
- * BID: 24524
<http://www.securityfocus.com/bid/24524>
- * BID: 25159
<http://www.securityfocus.com/bid/25159>
- * VUPEN: ADV-2007-1729
<http://www.frsirt.com/english/advisories/2007/1729>
- * VUPEN: ADV-2007-2732
<http://www.frsirt.com/english/advisories/2007/2732>
- * VUPEN: ADV-2007-3087
<http://www.frsirt.com/english/advisories/2007/3087>
- * VUPEN: ADV-2007-3386
<http://www.frsirt.com/english/advisories/2007/3386>
- * VUPEN: ADV-2008-1979
<http://www.frsirt.com/english/advisories/2008/1979/references>
- * VUPEN: ADV-2009-0233
<http://www.frsirt.com/english/advisories/2009/0233>
- * SECTRAK: 1018269

<http://www.securitytracker.com/id?1018269>

* SECUNIA: 25721

<http://secunia.com/advisories/25721>

* SECUNIA: 26235

<http://secunia.com/advisories/26235>

* SECUNIA: 26660

<http://secunia.com/advisories/26660>

* SECUNIA: 27037

<http://secunia.com/advisories/27037>

* SECUNIA: 27727

<http://secunia.com/advisories/27727>

* SECUNIA: 30908

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

* SECUNIA: 30899

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

* SECUNIA: 31493

<http://secunia.com/advisories/31493>

* SECUNIA: 33668

<http://secunia.com/advisories/33668>

CVE Reference:

CVE-2007-1358 (cve.mitre.org, nvd.nist.gov)

• 18638 Apache Tomcat Cross-site scripting Vulnerability (CVE-2006-7195)

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

The implicit-objects.jsp in the examples webapp displayed a number of unfiltered header values. This enabled a XSS attack. These values are now filtered.

The issue affects Apache Tomcat versions:

5.0.0-5.0.30

5.5.0-5.5.17

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

References:

* BUGTRAQ: 20080108 VMSA-2008-0002 Low severity security update for VirtualCenter and ESX Server 3.0.2, and ESX 3.0.1

<http://www.securityfocus.com/archive/1/archive/1/485938/100/0/threaded>

* BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)

<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>

* BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities

<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>

* MLIST: [Security-announce] 20080107 VMSA-2008-0002 Low severity security update for VirtualCenter and ESX Server 3.0.2, and ESX 3.0.1

<http://lists.vmware.com/pipermail/security-announce/2008/000003.html>

* CONFIRM:

<http://tomcat.apache.org/security-5.html>

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2007-206.htm>

* CONFIRM:

<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>

* CONFIRM:

<http://support.ca.com/iri/portal/anonymous/phpsupcontent?contentID=197540>

* REDHAT: RHSA-2007:0327

<http://www.redhat.com/support/errata/RHSA-2007-0327.html>

* REDHAT: RHSA-2008:0261

<http://www.redhat.com/support/errata/RHSA-2008-0261.html>

* BID: 28481

<http://www.securityfocus.com/bid/28481>

* VUPEN: ADV-2007-1729

<http://www.frsirt.com/english/advisories/2007/1729>

* VUPEN: ADV-2008-0065

<http://www.frsirt.com/english/advisories/2008/0065>

* VUPEN: ADV-2009-0233

<http://www.frsirt.com/english/advisories/2009/0233>

* SECUNIA: 28365

<http://secunia.com/advisories/28365>

* SECUNIA: 33668
<http://secunia.com/advisories/33668>

CVE Reference:

CVE-2006-7195 (cve.mitre.org, nvd.nist.gov)

• 18639 Apache Tomcat Information disclosure Vulnerability (CVE-2007-1858)

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

The default SSL configuration permitted the use of insecure cipher suites including the anonymous cipher suite. The default configuration no longer permits the use of insecure cipher suites.

The issue affects Apache Tomcat versions:

5.0.0-5.0.30
5.5.0-5.5.16
4.1.28-4.1.31

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

References:

- * BUGTRAQ: 20090127 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities (Updated - v1.1)
<http://www.securityfocus.com/archive/1/archive/1/500412/100/0/threaded>
- * BUGTRAQ: 20090124 CA20090123-01: Cohesion Tomcat Multiple Vulnerabilities
<http://www.securityfocus.com/archive/1/archive/1/500396/100/0/threaded>
- * CONFIRM:
<http://tomcat.apache.org/security-4.html>
- * CONFIRM:
<http://tomcat.apache.org/security-5.html>
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2007-206.htm>
- * CONFIRM:
<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>
- * CONFIRM:
<http://support.ca.com/iri/portal/anonymous/phpsupcontent?contentID=197540>
- * SUSE: SUSE-SR:2008:007
<http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00008.html>
- * BID: 28482
<http://www.securityfocus.com/bid/28482>
- * VUPEN: ADV-2007-1729
<http://www.frsirt.com/english/advisories/2007/1729>
- * VUPEN: ADV-2009-0233
<http://www.frsirt.com/english/advisories/2009/0233>
- * OSVDB: 34882
<http://osvdb.org/34882>
- * SECUNIA: 29392
<http://secunia.com/advisories/29392>
- * SECUNIA: 33668
<http://secunia.com/advisories/33668>
- * XF: tomcat-ssl-security-bypass(34212)
<http://xforce.iss.net/xforce/xfdb/34212>

CVE Reference:

CVE-2007-1858 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-4210 Microsoft CVSS 2.0 Score = 9.3

The Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted media content.

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

References:

MSKB: <http://support.microsoft.com/kb/976138>

XF: <http://xforce.iss.net/xforce/xfdb/54645>

XF: <http://xforce.iss.net/xforce/xfdb/54644>

VUPEN: <http://www.vupen.com/english/advisories/2009/3440>

BID: <http://www.securityfocus.com/bid/37251>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/508323/100/0/threaded>

OSVDB: <http://www.osvdb.org/60857>

CONFIRM: <http://www.microsoft.com/technet/security/advisory/954157.mspx>

MISC: <http://www.fortiguard.com/advisory/FGA-2009-45.html>

MSKB: <http://support.microsoft.com/kb/955759>

MSKB: <http://support.microsoft.com/kb/954157>

SECTRAK: <http://securitytracker.com/id?1023302>

SECUNIA: <http://secunia.com/advisories/37592>

CVE Reference: [CVE-2009-4210](#)

• **CVE-2009-4309 Microsoft CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in the Intel Indeo41 codec for Windows Media Player in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via a large size value in a movi record in an IV41 stream in a media file, as demonstrated by an AVI file.

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

References:

CONFIRM: <http://www.microsoft.com/technet/security/advisory/954157.mspx>

MSKB: <http://support.microsoft.com/kb/976138>

MSKB: <http://support.microsoft.com/kb/955759>

MSKB: <http://support.microsoft.com/kb/954157>

SECTRAK: <http://securitytracker.com/id?1023302>

MISC: <http://zerodayinitiative.com/advisories/ZDI-09-089/>

XF: <http://xforce.iss.net/xforce/xfdb/54645>

XF: <http://xforce.iss.net/xforce/xfdb/54642>

VUPEN: <http://www.vupen.com/english/advisories/2009/3440>

BID: <http://www.securityfocus.com/bid/37251>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/508324/100/0/threaded>

OSVDB: <http://www.osvdb.org/60855>

SECUNIA: <http://secunia.com/advisories/37592>

CVE Reference: [CVE-2009-4309](#)

• **CVE-2009-4310 Microsoft CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in the Intel Indeo41 codec for Windows Media Player in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted compressed video data in an IV41 stream in a media file, leading to many loop iterations, as demonstrated by data in an AVI file.

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

References:

CONFIRM: <http://www.microsoft.com/technet/security/advisory/954157.msp>

MSKB: <http://support.microsoft.com/kb/976138>

MSKB: <http://support.microsoft.com/kb/955759>

MSKB: <http://support.microsoft.com/kb/954157>

SECTRAK: <http://securitytracker.com/id?1023302>

MISC: <http://zerodayinitiative.com/advisories/ZDI-09-090/>

XF: <http://xforce.iss.net/xforce/xfdb/54645>

XF: <http://xforce.iss.net/xforce/xfdb/54643>

VUPEN: <http://www.vupen.com/english/advisories/2009/3440>

BID: <http://www.securityfocus.com/bid/37251>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/508335/100/0/threaded>

OSVDB: <http://www.osvdb.org/60856>

SECUNIA: <http://secunia.com/advisories/37592>

CVE Reference: [CVE-2009-4310](#)

• **CVE-2009-4311 Microsoft CVSS 2.0 Score = 9.3**

Unspecified vulnerability in the Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted media content, as reported to Microsoft by Paul Byrne of NGS Software. NOTE: this might overlap CVE-2008-3615.

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

References:

CONFIRM: <http://www.microsoft.com/technet/security/advisory/954157.msp>

MSKB: <http://support.microsoft.com/kb/976138>

MSKB: <http://support.microsoft.com/kb/955759>

MSKB: <http://support.microsoft.com/kb/954157>

XF: <http://xforce.iss.net/xforce/xfdb/54645>

VUPEN: <http://www.vupen.com/english/advisories/2009/3440>

BID: <http://www.securityfocus.com/bid/37251>

SECTRAK: <http://securitytracker.com/id?1023302>

SECUNIA: <http://secunia.com/advisories/37592>

CVE Reference: [CVE-2009-4311](#)

• **CVE-2009-4312 Microsoft CVSS 2.0 Score = 9.3**

Unspecified vulnerability in the Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted media content, as reported to Microsoft by Dave Lenoe of Adobe.

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

References:

CONFIRM: <http://www.microsoft.com/technet/security/advisory/954157.msp>

MSKB: <http://support.microsoft.com/kb/976138>

MSKB: <http://support.microsoft.com/kb/955759>

MSKB: <http://support.microsoft.com/kb/954157>

XF: <http://xforce.iss.net/xforce/xfdb/54645>

VUPEN: <http://www.vupen.com/english/advisories/2009/3440>

BID: <http://www.securityfocus.com/bid/37251>

SECTRAK: <http://securitytracker.com/id?1023302>

SECUNIA: <http://secunia.com/advisories/37592>

CVE Reference: [CVE-2009-4312](#)

• **CVE-2009-4313 Microsoft CVSS 2.0 Score = 9.3**

ir32_32.dll 3.24.15.3 in the Indeo32 codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to cause a denial of service (heap corruption) or execute arbitrary code via malformed data in a stream in a media file, as demonstrated by an AVI file.

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

References:

CONFIRM: <http://www.microsoft.com/technet/security/advisory/954157.msp>

MSKB: <http://support.microsoft.com/kb/976138>

MSKB: <http://support.microsoft.com/kb/955759>

MSKB: <http://support.microsoft.com/kb/954157>

XF: <http://xforce.iss.net/xforce/xfdb/54645>

VUPEN: <http://www.vupen.com/english/advisories/2009/3440>

BID: <http://www.securityfocus.com/bid/37251>

OSVDB: <http://www.osvdb.org/60858>

SECTRAK: <http://securitytracker.com/id?1023302>

SECUNIA: <http://secunia.com/advisories/37592>

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=835>

CVE Reference: [CVE-2009-4313](#)

• **CVE-2009-4335 IBM CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in bundled stored procedures in the Spatial Extender component in IBM DB2 9.5 before FP5 have unknown impact and remote attack vectors, related to "remote exploits."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/3520>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21293566>

BID: <http://www.securityfocus.com/bid/37332>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21412902>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1IC62625>

SECUNIA: <http://secunia.com/advisories/37759>

CONFIRM: ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v95/APARLIST.TXT

CVE Reference: [CVE-2009-4335](#)

• **CVE-2009-4333 IBM CVSS 2.0 Score = 7.5**

The Relational Data Services component in IBM DB2 9.5 before FP5 allows attackers to obtain the password argument from the SET ENCRYPTION PASSWORD statement via vectors involving the GET SNAPSHOT FOR DYNAMIC SQL command.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21293566>

VUPEN: <http://www.vupen.com/english/advisories/2009/3520>

BID: <http://www.securityfocus.com/bid/37332>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21412902>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11Z38819>

SECUNIA: <http://secunia.com/advisories/37759>

CONFIRM: ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v95/APARLIST.TXT

CVE Reference: [CVE-2009-4333](#)

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