

## 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>

[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

The White House has new Cybersecurity coordinator. DNS service attacked. New products to protect smartphones. netVigilance wishes all a happy and prosperous New Year.

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

### • President Obama greets new cybersecurity chief

Several key areas are to be addressed by Howard Schmidt as he begins his new job as the cybersecurity coordinator to the White House.

In a video address from the White House, Schmidt said he was honored to have been selected by President Obama and said that daily dependence on information technologies "present us with great opportunity and great danger."

Schmidt said, "Our lives have been enriched with technologies that are now part of the very fabric of our day-to-day

lives, our dependence on these wonderful technologies continue to increase with each innovation as does our responsibility to protect our security and our privacy. SC Magazine

Full Story :

[http://www.scmagazineus.com/president-obama-greets-new-cybersecurity-chief/article/160249/?utm\\_source=feedbu](http://www.scmagazineus.com/president-obama-greets-new-cybersecurity-chief/article/160249/?utm_source=feedbu)

### • DDoS attack hobbles major sites, including Amazon

People flocked to Google Wednesday evening to figure out what was happening with the UltraDNS service, which suffered a DDoS attack at the height of the last-minute shopping season.

(Credit: Screenshot by Tom Krazit/CNET) An attack directed at the DNS provider for some of the Internet's larger e-commerce companies--including Amazon, Wal-Mart, and Expedia--took several Internet shopping sites offline Wednesday evening, two days before Christmas.

Neustar, the company that provides DNS services under the UltraDNS brand name, confirmed an attack took place Wednesday afternoon, taking out sites or rendering them extremely sluggish for about an hour. A representative who answered the customer support line said the attacks were directed against Neustar facilities in Palo Alto and San Jose, Calif., and Allen Goldberg, vice president of corporate communications for Neustar, confirmed that at about 4:45 p.m. PST, "our alarms went off." Cnet Security

Full Story :

[http://news.cnet.com/8301-30684\\_3-10421577-265.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-30684_3-10421577-265.html?part=rss&subj=news&tag=2547-1_3-0-20)

### • Web-based Lookout protects mobile devices, data

John Hering, co-founder and chief executive of Lookout

(Credit: James Martin/CNET )

SAN FRANCISCO--In July, John Hering and Kevin Mahaffey demonstrated an SMS attack targeting a variety of smartphones at a security show. This week they are launching a company, with backing from some heavyweight investors, that will offer a fix for that problem, as well as protect smartphones from many other security issues. Cnet Security

Full Story :

[http://news.cnet.com/8301-27080\\_3-10421525-245.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-27080_3-10421525-245.html?part=rss&subj=news&tag=2547-1_3-0-20)

## New Vulnerabilities Tested in SecureScout

### • 18650 OpenSSL dtls1\_buffer\_record Denial of Service Vulnerability

The dtls1\_buffer\_record function in ssl/d1\_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."

Users of OpenSSL 0.9.8 on affected platforms should update to 0.9.8l which contains a patch to correct this issue.

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

#### References:

\* MLIST: [openssl-dev] 20090516 [openssl.org #1930] [PATCH] DTLS record buffer limitation bug

<http://marc.info/?l=openssl-dev&m=124247675613888&w=2>

\* MLIST: [oss-security] 20090518 Two OpenSSL DTLS remote DoS

<http://www.openwall.com/lists/oss-security/2009/05/18/1>

\* MISC:

<https://launchpad.net/bugs/cve/2009-1377>

\* CONFIRM:

<http://cvs.openssl.org/chngview?cn=18187>

\* CONFIRM:

<http://rt.openssl.org/Ticket/Display.html?id=1930&user=quest&pass=quest>

\* CONFIRM:

[http://sourceforge.net/mailarchive/message.php?msg\\_name=4AD43807.7080105%40users.sourceforge.net](http://sourceforge.net/mailarchive/message.php?msg_name=4AD43807.7080105%40users.sourceforge.net)

\* CONFIRM:

<http://voodoo-circle.sourceforge.net/sa/sa-20091012-01.html>

\* GENTOO: GLSA-200912-01

<http://security.gentoo.org/glsa/glsa-200912-01.xml>

\* MANDRIVA: MDVSA-2009:120

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:120>

\* NETBSD: NetBSD-SA2009-009  
ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2009-009.txt.asc  
\* SUSE: SUSE-SR:2009:011  
<http://lists.opensuse.org/opensuse-security-announce/2009-06/msg00003.html>  
\* UBUNTU: USN-792-1  
<http://www.ubuntu.com/usn/USN-792-1>  
\* BID: 35001  
<http://www.securityfocus.com/bid/35001>  
\* SECTRACK: 1022241  
<http://www.securitytracker.com/id?1022241>  
\* SECUNIA: 35128  
<http://secunia.com/advisories/35128>  
\* SECUNIA: 35416  
<http://secunia.com/advisories/35416>  
\* SECUNIA: 35461  
<http://secunia.com/advisories/35461>  
\* SECUNIA: 35571  
<http://secunia.com/advisories/35571>  
\* SECUNIA: 35729  
<http://secunia.com/advisories/35729>  
\* SECUNIA: 37003  
<http://secunia.com/advisories/37003>  
\* VUPEN: ADV-2009-1377  
<http://www.vupen.com/english/advisories/2009/1377>

#### CVE Reference:

CVE-2009-1377 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18651 OpenSSL dtls1\_process\_out\_of\_seq\_message Denial of Service Vulnerability

Multiple memory leaks in the dtls1\_process\_out\_of\_seq\_message function in ssl/d1\_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."

Users of OpenSSL 0.9.8 on affected platforms should update to 0.9.8l which contains a patch to correct this issue.

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

#### References:

\* MILWORM: 8720  
<http://www.milw0rm.com/exploits/8720>  
\* MLIST: [openssl-dev] 20090516 [openssl.org #1931] [PATCH] DTLS fragment handling memory leak  
<http://marc.info/?l=openssl-dev&m=124247679213944&w=2>  
\* MLIST: [openssl-dev] 20090518 Re: [openssl.org #1931] [PATCH] DTLS fragment handling memory leak  
<http://marc.info/?l=openssl-dev&m=124263491424212&w=2>  
\* MLIST: [oss-security] 20090518 Two OpenSSL DTLS remote DoS  
<http://www.openwall.com/lists/oss-security/2009/05/18/1>  
\* MISC:  
<https://launchpad.net/bugs/cve/2009-1378>  
\* CONFIRM:  
<http://cvs.openssl.org/chngview?cn=18188>  
\* CONFIRM:  
<http://rt.openssl.org/Ticket/Display.html?id=1931&user=guest&pass=guest>  
\* CONFIRM:  
[http://sourceforge.net/mailarchive/message.php?msg\\_name=4AD43807.7080105%40users.sourceforge.net](http://sourceforge.net/mailarchive/message.php?msg_name=4AD43807.7080105%40users.sourceforge.net)  
\* CONFIRM:  
<http://voodoo-circle.sourceforge.net/sa/sa-20091012-01.html>  
\* GENTOO: GLSA-200912-01  
<http://security.gentoo.org/glsa/glsa-200912-01.xml>  
\* MANDRIVA: MDVSA-2009:120  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:120>  
\* NETBSD: NetBSD-SA2009-009  
ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2009-009.txt.asc  
\* SUSE: SUSE-SR:2009:011  
<http://lists.opensuse.org/opensuse-security-announce/2009-06/msg00003.html>  
\* UBUNTU: USN-792-1  
<http://www.ubuntu.com/usn/USN-792-1>  
\* BID: 35001

<http://www.securityfocus.com/bid/35001>  
\* SECTRACK: 1022241  
<http://www.securitytracker.com/id?1022241>  
\* SECUNIA: 35128  
<http://secunia.com/advisories/35128>  
\* SECUNIA: 35416  
<http://secunia.com/advisories/35416>  
\* SECUNIA: 35461  
<http://secunia.com/advisories/35461>  
\* SECUNIA: 35571  
<http://secunia.com/advisories/35571>  
\* SECUNIA: 35729  
<http://secunia.com/advisories/35729>  
\* SECUNIA: 37003  
<http://secunia.com/advisories/37003>  
\* VUPEN: ADV-2009-1377  
<http://www.vupen.com/english/advisories/2009/1377>

#### CVE Reference:

CVE-2009-1378 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18654 Apache Tomcat Session hi-jacking Vulnerability (CVE-2007-5333)

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

Apache Tomcat 6.0.0 through 6.0.14, 5.5.0 through 5.5.25, and 4.1.0 through 4.1.36 does not properly handle (1) double quote (") characters or (2) %5C (encoded backslash) sequences in a cookie value, which might cause sensitive information such as session IDs to be leaked to remote attackers and enable session hijacking attacks. NOTE: this issue exists because of an incomplete fix for CVE-2007-3385.

The issue affects Apache Tomcat versions:

4.1.0-4.1.36  
5.5.0-5.5.25  
6.0.0-6.0.14

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

#### References:

\* BUGTRAQ: 20080208 [SECURITY] CVE-2007-5333: Tomcat Cookie handling vulnerabilities  
<http://www.securityfocus.com/archive/1/archive/1/487822/100/0/threaded>  
\* BUGTRAQ: 20091120 VMSA-2009-0016 VMware vCenter and ESX update release and vMA patch release address multiple security issue in third party components  
<http://www.securityfocus.com/archive/1/archive/1/507985/100/0/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://www.vmware.com/security/advisories/VMSA-2008-0010.html>  
\* CONFIRM:  
<http://support.apple.com/kb/HT2163>  
\* CONFIRM:  
<http://www-01.ibm.com/support/docview.wss?uid=swg24018932>  
\* CONFIRM:  
<http://support.apple.com/kb/HT3216>  
\* CONFIRM:  
<http://www-01.ibm.com/support/docview.wss?uid=swg27012047>  
\* CONFIRM:  
<http://www-01.ibm.com/support/docview.wss?uid=swg27012048>  
\* CONFIRM:  
<http://www.vmware.com/security/advisories/VMSA-2009-0016.html>  
\* CONFIRM:  
[http://www.redhat.com/docs/en-US/JBoss\\_Enterprise\\_Application\\_Platform/4.2.0.cp08/html-single/Release\\_Notes/index.html](http://www.redhat.com/docs/en-US/JBoss_Enterprise_Application_Platform/4.2.0.cp08/html-single/Release_Notes/index.html)  
\* CONFIRM:  
[https://bugzilla.redhat.com/show\\_bug.cgi?id=532111](https://bugzilla.redhat.com/show_bug.cgi?id=532111)  
\* AIXAPAR: IZ20991  
<http://www-1.ibm.com/support/docview.wss?uid=swg1IZ20991>

\* AIXAPAR: IZ20133  
<http://www-1.ibm.com/support/docview.wss?uid=swg1IZ20133>

\* APPLE: APPLE-SA-2008-06-30  
<http://lists.apple.com/archives/security-announce/2008/Jun/msg00002.html>

\* APPLE: APPLE-SA-2008-10-09  
<http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html>

\* FEDORA: FEDORA-2008-1467  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00315.html>

\* FEDORA: FEDORA-2008-1603  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00460.html>

\* GENTOO: GLSA-200804-10  
<http://security.gentoo.org/glsa-200804-10.xml>

\* MANDRIVA: MDVSA-2009:018  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:018>

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

\* JVN: JVN#09470767  
<http://jvn.jp/jp/JVN%2309470767/index.html>

\* BID: 27706  
<http://www.securityfocus.com/bid/27706>

\* BID: 31681  
<http://www.securityfocus.com/bid/31681>

\* SECUNIA: 37460  
<http://secunia.com/advisories/37460>

\* VUPEN: ADV-2008-0488  
<http://www.frsirt.com/english/advisories/2008/0488>

\* VUPEN: ADV-2008-1856  
<http://www.frsirt.com/english/advisories/2008/1856/references>

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

\* VUPEN: ADV-2008-2780  
<http://www.frsirt.com/english/advisories/2008/2780>

\* VUPEN: ADV-2008-2690  
<http://www.frsirt.com/english/advisories/2008/2690>

\* SECUNIA: 28878  
<http://secunia.com/advisories/28878>

\* SECUNIA: 28884  
<http://secunia.com/advisories/28884>

\* SECUNIA: 28915  
<http://secunia.com/advisories/28915>

\* SECUNIA: 29711  
<http://secunia.com/advisories/29711>

\* SECUNIA: 30676  
<http://secunia.com/advisories/30676>

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

\* SECUNIA: 32036  
<http://secunia.com/advisories/32036>

\* SECUNIA: 32222  
<http://secunia.com/advisories/32222>

\* SECUNIA: 33330  
<http://secunia.com/advisories/33330>

\* SREASON: 3636  
<http://securityreason.com/securityalert/3636>

\* VUPEN: ADV-2009-3316  
<http://www.vupen.com/english/advisories/2009/3316>

#### CVE Reference:

CVE-2007-5333 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18655 Apache Tomcat Elevated privileges Vulnerability (CVE-2007-5342)

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

The JULI logging component allows web applications to provide their own logging configurations. The default security policy does not restrict this configuration and allows an untrusted web application to add files or overwrite existing files where the Tomcat process has the necessary file permissions to do so.

The issue affects Apache Tomcat versions:  
5.5.9-5.5.25

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

## References:

- \* BUGTRAQ: 20071223 [CVE-2007-5342] Apache Tomcat's default security policy is too open  
<http://www.securityfocus.com/archive/1/archive/1/485481/100/0/threaded>
- \* BUGTRAQ: 20091120 VMSA-2009-0016 VMware vCenter and ESX update release and vMA patch release address multiple security issue in third party components  
<http://www.securityfocus.com/archive/1/archive/1/507985/100/0/threaded>
- \* MISC:  
<http://svn.apache.org/viewvc?view=rev&revision=606594>
- \* CONFIRM:  
<http://tomcat.apache.org/security-5.html>
- \* CONFIRM:  
<http://tomcat.apache.org/security-6.html>
- \* CONFIRM:  
<http://www.vmware.com/security/advisories/VMSA-2008-0010.html>
- \* CONFIRM:  
<http://support.apple.com/kb/HT3216>
- \* CONFIRM:  
<http://support.avaya.com/elmodocs2/security/ASA-2008-401.htm>
- \* CONFIRM:  
<http://www.vmware.com/security/advisories/VMSA-2009-0016.html>
- \* APPLE: APPLE-SA-2008-10-09  
<http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html>
- \* DEBIAN: DSA-1447  
<http://www.debian.org/security/2008/dsa-1447>
- \* FEDORA: FEDORA-2008-1467  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00315.html>
- \* FEDORA: FEDORA-2008-1603  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00460.html>
- \* GENTOO: GLSA-200804-10  
<http://security.gentoo.org/glsa/glsa-200804-10.xml>
- \* MANDRIVA: MDVSA-2008:188  
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:188>
- \* REDHAT: RHSA-2008:0042  
<http://www.redhat.com/support/errata/RHSA-2008-0042.html>
- \* REDHAT: RHSA-2008:0195  
<http://www.redhat.com/support/errata/RHSA-2008-0195.html>
- \* REDHAT: RHSA-2008:0862  
<http://www.redhat.com/support/errata/RHSA-2008-0862.html>
- \* REDHAT: RHSA-2008:0831  
<http://www.redhat.com/support/errata/RHSA-2008-0831.html>
- \* REDHAT: RHSA-2008:0832  
<http://www.redhat.com/support/errata/RHSA-2008-0832.html>
- \* REDHAT: RHSA-2008:0833  
<http://www.redhat.com/support/errata/RHSA-2008-0833.html>
- \* REDHAT: RHSA-2008:0834  
<http://www.redhat.com/support/errata/RHSA-2008-0834.html>
- \* SUSE: SUSE-SR:2009:004  
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>
- \* BID: 27006  
<http://www.securityfocus.com/bid/27006>
- \* BID: 31681  
<http://www.securityfocus.com/bid/31681>
- \* SECUNIA: 37460  
<http://secunia.com/advisories/37460>
- \* VUPEN: ADV-2008-0013  
<http://www.frsirt.com/english/advisories/2008/0013>
- \* VUPEN: ADV-2008-1856  
<http://www.frsirt.com/english/advisories/2008/1856/references>
- \* VUPEN: ADV-2008-2823  
<http://www.frsirt.com/english/advisories/2008/2823>
- \* VUPEN: ADV-2008-2780  
<http://www.frsirt.com/english/advisories/2008/2780>
- \* OSVDB: 39833  
<http://osvdb.org/39833>
- \* SECUNIA: 28274

<http://secunia.com/advisories/28274>

\* SECUNIA: 28317

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

\* SECUNIA: 28915

<http://secunia.com/advisories/28915>

\* SECUNIA: 29313

<http://secunia.com/advisories/29313>

\* SECUNIA: 29711

<http://secunia.com/advisories/29711>

\* SECUNIA: 30676

<http://secunia.com/advisories/30676>

\* SECUNIA: 32222

<http://secunia.com/advisories/32222>

\* SECUNIA: 32120

<http://secunia.com/advisories/32120>

\* SECUNIA: 32266

<http://secunia.com/advisories/32266>

\* SREASON: 3485

<http://securityreason.com/securityalert/3485>

\* VUPEN: ADV-2009-3316

<http://www.vupen.com/english/advisories/2009/3316>

\* XF: apache-juli-logging-weak-security(39201)

<http://xforce.iss.net/xforce/xfdb/39201>

#### CVE Reference:

CVE-2007-5342 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18656 Apache Tomcat Information disclosure Vulnerability (CVE-2007-5461)

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

When Tomcat's WebDAV servlet is configured for use with a context and has been enabled for write, some WebDAV requests that specify an entity with a SYSTEM tag can result in the contents of arbitrary files being returned to the client.

The issue affects Apache Tomcat versions:

4.0.0-4.0.6

4.1.0-4.1.36

5.5.0-5.5.25

6.0.0-6.0.14

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

#### References:

\* BUGTRAQ: 20091120 VMSA-2009-0016 VMware vCenter and ESX update release and vMA patch release address multiple security issue in third party components

<http://www.securityfocus.com/archive/1/archive/1/507985/100/0/threaded>

\* FULLDISC: 20071014 Apache Tomcat Remote File Disclosure ZeroDay

<http://marc.info/?l=full-disclosure&m=119239530508382>

\* MILWORM: 4530

<http://www.milw0rm.com/exploits/4530>

\* MLIST: [tomcat-users] 20071015 [Security] - Important vulnerability disclosed in Apache Tomcat webdav servlet

[http://mail-archives.apache.org/mod\\_mbox/tomcat-users/200710.mbox/%3C47135C2D.1000705@apache.org%3E](http://mail-archives.apache.org/mod_mbox/tomcat-users/200710.mbox/%3C47135C2D.1000705@apache.org%3E)

\* MISC:

<http://issues.apache.org/jira/browse/GERONIMO-3549>

\* 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://geronimo.apache.org/2007/10/18/potential-vulnerability-in-apache-tomcat-webdav-servlet.html>

\* CONFIRM:

<http://www-1.ibm.com/support/docview.wss?uid=swg21286112>

\* CONFIRM:

<http://www.vmware.com/security/advisories/VMSA-2008-0010.html>

\* CONFIRM:

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

\* CONFIRM:  
<http://support.apple.com/kb/HT3216>

\* CONFIRM:  
<http://support.avaya.com/elmodocs2/security/ASA-2008-401.htm>

\* CONFIRM:  
<http://www.vmware.com/security/advisories/VMSA-2009-0016.html>

\* APPLE: APPLE-SA-2008-06-30  
<http://lists.apple.com/archives/security-announce/2008/Jun/msg00002.html>

\* APPLE: APPLE-SA-2008-10-09  
<http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.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>

\* GENTOO: GLSA-200804-10  
<http://security.gentoo.org/glsa/glsa-200804-10.xml>

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

\* MANDRIVA: MDVSA-2009:136  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:136>

\* REDHAT: RHSA-2008:0042  
<http://www.redhat.com/support/errata/RHSA-2008-0042.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>

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

\* REDHAT: RHSA-2008:0862  
<http://www.redhat.com/support/errata/RHSA-2008-0862.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>

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

\* BID: 26070  
<http://www.securityfocus.com/bid/26070>

\* BID: 31681  
<http://www.securityfocus.com/bid/31681>

\* SECUNIA: 37460  
<http://secunia.com/advisories/37460>

\* VUPEN: ADV-2007-3622  
<http://www.frsirt.com/english/advisories/2007/3622>

\* VUPEN: ADV-2007-3671  
<http://www.frsirt.com/english/advisories/2007/3671>

\* VUPEN: ADV-2007-3674  
<http://www.frsirt.com/english/advisories/2007/3674>

\* VUPEN: ADV-2008-1856  
<http://www.frsirt.com/english/advisories/2008/1856/references>

\* 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-2008-2823  
<http://www.frsirt.com/english/advisories/2008/2823>

\* VUPEN: ADV-2008-2780  
<http://www.frsirt.com/english/advisories/2008/2780>

\* SECTRACK: 1018864  
<http://www.securitytracker.com/id?1018864>

\* SECUNIA: 27398  
<http://secunia.com/advisories/27398>

\* SECUNIA: 27446  
<http://secunia.com/advisories/27446>

\* SECUNIA: 27481  
<http://secunia.com/advisories/27481>

\* 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: 29313

<http://secunia.com/advisories/29313>

\* SECUNIA: 29711

<http://secunia.com/advisories/29711>

\* SECUNIA: 30676

<http://secunia.com/advisories/30676>

\* 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: 32222

<http://secunia.com/advisories/32222>

\* SECUNIA: 32120

<http://secunia.com/advisories/32120>

\* SECUNIA: 32266

<http://secunia.com/advisories/32266>

\* VUPEN: ADV-2009-3316

<http://www.vupen.com/english/advisories/2009/3316>

\* XF: apache-tomcat-webdav-dir-traversal(37243)

<http://xforce.iss.net/xforce/xfdb/37243>

#### CVE Reference:

CVE-2007-5461 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18657 Apache Tomcat Data integrity Vulnerability (CVE-2007-6286)

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

When using the native (APR based) connector, connecting to the SSL port using netcat and then disconnecting without sending any data will cause tomcat to handle a duplicate copy of one of the recent requests.

The issue affects Apache Tomcat versions:

5.5.11-5.5.25

6.0.0-6.0.15

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

#### References:

\* BUGTRAQ: 20080208 [SECURITY] CVE-2007-6286: Tomcat duplicate request processing vulnerability

<http://www.securityfocus.com/archive/1/archive/1/487823/100/0/threaded>

\* BUGTRAQ: 20091120 VMSA-2009-0016 VMware vCenter and ESX update release and vMA patch release address multiple security issue in third party components

<http://www.securityfocus.com/archive/1/archive/1/507985/100/0/threaded>

\* CONFIRM:

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

\* CONFIRM:

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

\* CONFIRM:

<http://www.vmware.com/security/advisories/VMSA-2008-0010.html>

\* CONFIRM:

<http://support.apple.com/kb/HT3216>

\* CONFIRM:

<http://www.vmware.com/security/advisories/VMSA-2009-0016.html>

\* APPLE: APPLE-SA-2008-10-09

<http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html>

\* FEDORA: FEDORA-2008-1467

<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00315.html>

\* FEDORA: FEDORA-2008-1603

<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00460.html>  
\* GENTOO: GLSA-200804-10  
<http://security.gentoo.org/glsa/glsa-200804-10.xml>  
\* MANDRIVA: MDVSA-2009:136  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:136>  
\* SUSE: SUSE-SR:2009:004  
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>  
\* BID: 31681  
<http://www.securityfocus.com/bid/31681>  
\* SECUNIA: 37460  
<http://secunia.com/advisories/37460>  
\* VUPEN: ADV-2008-0488  
<http://www.frsirt.com/english/advisories/2008/0488>  
\* VUPEN: ADV-2008-1856  
<http://www.frsirt.com/english/advisories/2008/1856/references>  
\* VUPEN: ADV-2008-2780  
<http://www.frsirt.com/english/advisories/2008/2780>  
\* SECUNIA: 28878  
<http://secunia.com/advisories/28878>  
\* SECUNIA: 28915  
<http://secunia.com/advisories/28915>  
\* SECUNIA: 29711  
<http://secunia.com/advisories/29711>  
\* SECUNIA: 30676  
<http://secunia.com/advisories/30676>  
\* SECUNIA: 32222  
<http://secunia.com/advisories/32222>  
\* SREASON: 3637  
<http://securityreason.com/securityalert/3637>  
\* VUPEN: ADV-2009-3316  
<http://www.vupen.com/english/advisories/2009/3316>

#### CVE Reference:

CVE-2007-6286 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18658 Apache Tomcat Information disclosure Vulnerability (CVE-2008-0002)

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

If an exception occurs during the processing of parameters (eg if the client disconnects) then it is possible that the parameters submitted for that request will be incorrectly processed as part of a subsequent request.

The issue affects Apache Tomcat versions:  
6.0.5-6.0.15

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

#### References:

\* BUGTRAQ: 20080208 CVE-2008-0002: Tomcat information disclosure vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/487812/100/0/threaded>  
\* BUGTRAQ: 20091120 VMSA-2009-0016 VMware vCenter and ESX update release and vMA patch release address multiple security issue in third party components  
<http://www.securityfocus.com/archive/1/archive/1/507985/100/0/threaded>  
\* CONFIRM:  
<http://tomcat.apache.org/security-6.html>  
\* CONFIRM:  
<http://support.apple.com/kb/HT3216>  
\* CONFIRM:  
<http://www.vmware.com/security/advisories/VMSA-2009-0016.html>  
\* APPLE: APPLE-SA-2008-10-09  
<http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html>  
\* FEDORA: FEDORA-2008-1467  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00315.html>  
\* FEDORA: FEDORA-2008-1603  
<https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00460.html>  
\* GENTOO: GLSA-200804-10  
<http://security.gentoo.org/glsa/glsa-200804-10.xml>  
\* SUSE: SUSE-SR:2009:004  
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>

\* BID: 27703  
<http://www.securityfocus.com/bid/27703>  
\* BID: 31681  
<http://www.securityfocus.com/bid/31681>  
\* SECUNIA: 37460  
<http://secunia.com/advisories/37460>  
\* VUPEN: ADV-2008-0488  
<http://www.frsirt.com/english/advisories/2008/0488>  
\* VUPEN: ADV-2008-2780  
<http://www.frsirt.com/english/advisories/2008/2780>  
\* SECUNIA: 28834  
<http://secunia.com/advisories/28834>  
\* SECUNIA: 28915  
<http://secunia.com/advisories/28915>  
\* SECUNIA: 29711  
<http://secunia.com/advisories/29711>  
\* SECUNIA: 32222  
<http://secunia.com/advisories/32222>  
\* SREASON: 3638  
<http://securityreason.com/securityalert/3638>  
\* VUPEN: ADV-2009-3316  
<http://www.vupen.com/english/advisories/2009/3316>

#### CVE Reference:

CVE-2008-0002 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### ● 18659 Apache Tomcat Cross-site scripting Vulnerability (CVE-2007-3386)

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

The Host Manager Servlet did not filter user supplied data before display. This enabled an XSS attack.

The issue affects Apache Tomcat versions:

6.0.0-6.0.13

5.5.0-5.5.24

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

#### References:

\* BUGTRAQ: 20070814 CVE-2007-3386: XSS in Host Manager  
<http://www.securityfocus.com/archive/1/archive/1/476448/100/0/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://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>  
\* CONFIRM:  
<http://support.ca.com/iri/portal/anonymous/phpsupcontent?contentID=197540>  
\* DEBIAN: DSA-1447  
<http://www.debian.org/security/2008/dsa-1447>  
\* 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>  
\* SUSE: SUSE-SR:2009:004  
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>  
\* JVN: JVN#59851336  
<http://jvn.jp/jp/JVN%2359851336/index.html>  
\* BID: 25314  
<http://www.securityfocus.com/bid/25314>

\* VUPEN: ADV-2007-2880  
<http://www.frsirt.com/english/advisories/2007/2880>  
\* 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-2009-0233  
<http://www.frsirt.com/english/advisories/2009/0233>  
\* OSVDB: 36417  
<http://osvdb.org/36417>  
\* SECTRACK: 1018558  
<http://securitytracker.com/id?1018558>  
\* SECUNIA: 26465  
<http://secunia.com/advisories/26465>  
\* 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: 33668  
<http://secunia.com/advisories/33668>  
\* SREASON: 3010  
<http://securityreason.com/securityalert/3010>  
\* XF: tomcat-hostmanager-alias-xss(36001)  
<http://xforce.iss.net/xforce/xfdb/36001>

#### CVE Reference:

CVE-2007-3386 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18660 Apache Tomcat Information disclosure Vulnerability (CVE-2008-4308)

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

Bug 40771 may result in the disclosure of POSTed content from a previous request. For a vulnerability to exist, the content read from the input stream must be disclosed, eg via writing it to the response and committing the response, before the `ArrayIndexOutOfBoundsException` occurs which will halt processing of the request.

The issue affects Apache Tomcat versions:

5.5.10-5.5.20

4.1.32-4.1.34

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

#### References:

\* BUGTRAQ: 20090225 [SECURITY] CVE-2008-4308: Tomcat information disclosure vulnerability  
<http://www.securityfocus.com/archive/1/501250>  
\* MISC:  
[https://issues.apache.org/bugzilla/show\\_bug.cgi?id=40771](https://issues.apache.org/bugzilla/show_bug.cgi?id=40771)  
\* JVN: JVN#66905322  
<http://jvn.jp/en/jp/JVN66905322/index.html>  
\* JVNDB: JVNDB-2009-000010  
<http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-000010.html>  
\* BID: 33913  
<http://www.securityfocus.com/bid/33913>  
\* SECUNIA: 34057  
<http://secunia.com/advisories/34057>  
\* VUPEN: ADV-2009-0541  
<http://www.vupen.com/english/advisories/2009/0541>

#### CVE Reference:

CVE-2008-4308 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18661 Apache Tomcat Information disclosure Vulnerability (CVE-2008-3271)

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

Bug 25835 can, in rare circumstances - this has only been reproduced using a debugger to force a particular processing sequence for two threads - allow a user from a non-permitted IP address to gain access to a context that is protected with a valve that extends RequestFilterValve. This includes the standard RemoteAddrValve and RemoteHostValve implementations.

The issue affects Apache Tomcat versions:

5.5.0

4.1.0-4.1.31

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

#### References:

\* BUGTRAQ: 20081009 [SECURITY] CVE-2008-3271 - Apache Tomcat information disclosure

<http://www.securityfocus.com/archive/1/archive/1/497220/100/0/threaded>

\* CONFIRM:

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

\* CONFIRM:

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

\* CONFIRM:

<http://www.fujitsu.com/global/support/software/security/products-f/interstage-200806e.html>

\* CONFIRM:

[https://issues.apache.org/bugzilla/show\\_bug.cgi?id=25835](https://issues.apache.org/bugzilla/show_bug.cgi?id=25835)

\* CONFIRM:

<http://www.nec.co.jp/security-info/secinfo/nv09-006.html>

\* SUSE: SUSE-SR:2008:023

<http://lists.opensuse.org/opensuse-security-announce/2008-10/msg00012.html>

\* JVN: JVN#30732239

<http://jvn.jp/en/jp/JVN30732239/index.html>

\* JVNDB: JVNDB-2008-000069

<http://jvndb.jvn.jp/en/contents/2008/JVNDB-2008-000069.html>

\* BID: 31698

<http://www.securityfocus.com/bid/31698>

\* SECUNIA: 35684

<http://secunia.com/advisories/35684>

\* VUPEN: ADV-2008-2793

<http://www.frsirt.com/english/advisories/2008/2793>

\* VUPEN: ADV-2008-2800

<http://www.frsirt.com/english/advisories/2008/2800>

\* SECTRACK: 1021039

<http://www.securitytracker.com/id?1021039>

\* SECUNIA: 32234

<http://secunia.com/advisories/32234>

\* SECUNIA: 32213

<http://secunia.com/advisories/32213>

\* SECUNIA: 32398

<http://secunia.com/advisories/32398>

\* SREASON: 4396

<http://securityreason.com/securityalert/4396>

\* VUPEN: ADV-2009-1818

<http://www.vupen.com/english/advisories/2009/1818>

\* XF: apache-tomcat-valve-security-bypass(45791)

<http://xforce.iss.net/xforce/xfdb/45791>

#### CVE Reference:

CVE-2008-3271 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18640 Apache Tomcat Cross-site scripting Vulnerability (CVE-2006-7196)

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

The calendar application included as part of the JSP examples is susceptible to a cross-site scripting attack as it does not escape user provided data before including it in the returned page.

The issue affects Apache Tomcat versions:

5.0.0-5.0.30

5.5.0-5.5.15

4.0.0-4.0.6

4.1.0-4.1.31

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

#### References:

- \* BUGTRAQ: 20070904 Apache tomcat calendar example cross site scripting and cross site request forgery vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/478491/100/0/threaded>
- \* BUGTRAQ: 20070905 Re: Apache tomcat calendar example cross site scripting and cross site request forgery vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/478609/100/0/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://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-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>
- \* BID: 25531  
<http://www.securityfocus.com/bid/25531>
- \* 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: 34888  
<http://osvdb.org/34888>
- \* SECUNIA: 29242  
<http://secunia.com/advisories/29242>
- \* SECUNIA: 33668  
<http://secunia.com/advisories/33668>

#### CVE Reference:

CVE-2006-7196 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18641 Apache Tomcat Directory listing Vulnerability (CVE-2006-3835)

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

This is expected behavior when directory listings are enabled. The semicolon (;) is the separator for path parameters so inserting one before a file name changes the request into a request for a directory with a path parameter. If directory listings are enabled, a directory listing will be shown. In response to this and other directory listing issues, directory listings were changed to be disabled by default.

The issue affects Apache Tomcat versions:

5.0.0-5.0.30  
5.5.0-5.5.12  
4.0.0-4.0.6  
4.1.0-4.1.31

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

#### References:

- \* BUGTRAQ: 20070509 SEC Consult SA-20070509-0 :: Multiple vulnerabilities in Nokia Intellisync Mobile Suite & Wireless Email Express  
<http://www.securityfocus.com/archive/1/archive/1/468048/100/0/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>

\* FULLDISC: 20060721 Directory Listing in Apache Tomcat 5.x.x

<http://archives.neohapsis.com/archives/fulldisclosure/2006-07/0467.html>

\* MISC:

<http://www.sec-consult.com/289.html>

\* 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>

\* 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>

\* BID: 19106

<http://www.securityfocus.com/bid/19106>

\* VUPEN: ADV-2007-1727

<http://www.frsirt.com/english/advisories/2007/1727>

\* 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>

\* SECTRACK: 1016576

<http://securitytracker.com/id?1016576>

\* SECUNIA: 25212

<http://secunia.com/advisories/25212>

\* SECUNIA: 30908

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

\* SECUNIA: 30899

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

\* SECUNIA: 33668

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

\* XF: apache-tomcat-url-information-disclosure(27902)

<http://xforce.iss.net/xforce/xfdb/27902>

\* XF: nokia-tomcat-source-code-disclosure(34183)

<http://xforce.iss.net/xforce/xfdb/34183>

#### CVE Reference:

CVE-2006-3835 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18642 Apache Tomcat Denial of service Vulnerability (CVE-2005-3510)

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

The root cause is the relatively expensive calls required to generate the content for the directory listings. If directory listings are enabled, the number of files in each directory should be kept to a minimum. In response to this issue, directory listings were changed to be disabled by default. Additionally, a patch has been proposed that would improve performance, particularly for large directories, by caching directory listings.

The issue affects Apache Tomcat versions:

5.0.0-5.0.30

5.5.0-5.5.12

4.0.0-4.0.6

4.1.0-4.1.31

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

#### References:

\* BUGTRAQ: 20051104 Apache Tomcat 5.5.x remote Denial Of Service

<http://www.securityfocus.com/archive/1/archive/1/415782/30/0/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://community.ca.com/blogs/casecurityresponseblog/archive/2009/01/23.aspx>

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

\* REDHAT: RHSA-2006:0161  
<http://www.redhat.com/support/errata/RHSA-2006-0161.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>

\* BID: 15325  
<http://www.securityfocus.com/bid/15325>

\* 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: 20439  
<http://www.osvdb.org/20439>

\* SECTRAK: 1015147  
<http://securitytracker.com/id?1015147>

\* SECUNIA: 17416  
<http://secunia.com/advisories/17416>

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

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

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

#### CVE Reference:

CVE-2005-3510 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18643 Apache Tomcat Cross-site scripting Vulnerability (CVE-2005-4838)

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

Various JSPs included as part of the JSP examples and the Tomcat Manager are susceptible to a cross-site scripting attack as they do not escape user provided data before including it in the returned page.

The issue affects Apache Tomcat versions:

5.0.0-5.0.30  
5.5.0-5.5.6  
4.0.0-4.0.6  
4.1.0-4.1.31

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

#### References:

\* FULLDISC: 20070906 Apache Tomcat remote xss  
<http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/065598.html>

\* MISC:  
[http://www.oliverkarow.de/research/jakarta556\\_xss.txt](http://www.oliverkarow.de/research/jakarta556_xss.txt)

\* MLIST: [tomcat-dev] 20050103 Re: Fwd: XSS in Jakarta Tomcat 5.5.6  
<http://marc.info/?l=tomcat-dev&w=2>

\* MLIST: [tomcat-dev] 20050103 [PATCH jakarta-servletapi-5] Re: Fwd: XSS in Jakarta Tomcat 5.5.6  
<http://marc.info/?l=tomcat-dev&w=2>

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

\* CONFIRM:  
<http://tomcat.apache.org/security-5.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>

\* OSVDB: 12721

<http://www.osvdb.org/12721>

\* OSVDB: 34878

<http://www.osvdb.org/34878>

\* OSVDB: 34879

<http://www.osvdb.org/34879>

\* SECTRACK: 1012793

<http://securitytracker.com/id?1012793>

\* SECUNIA: 13737

<http://secunia.com/advisories/13737>

\* SECUNIA: 31493

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

\* XF: tomcat-functions-xss(36467)

<http://xforce.iss.net/xforce/xfdb/36467>

#### CVE Reference:

CVE-2005-4838 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18644 PHP mbstring extension arbitrary code execution Vulnerability

Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter\_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb\_convert\_encoding, (2) mb\_check\_encoding, (3) mb\_convert\_variables, and (4) mb\_parse\_str functions.

The issue has been fixed in PHP version 5.2.7.

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

#### References:

\* BUGTRAQ: 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl

<http://www.securityfocus.com/archive/1/archive/1/501376/100/0/threaded>

\* FULLDISC: 20081221 CVE-2008-5557 - PHP mbstring buffer overflow

<http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0477.html>

\* CONFIRM:

<http://bugs.php.net/bug.php?id=45722>

\* CONFIRM:

[http://cvs.php.net/viewvc.cgi/php-src/ext/mbstring/libmbfl/filters/mbfilter\\_htmlent.c?r1=1.7&r2=1.8](http://cvs.php.net/viewvc.cgi/php-src/ext/mbstring/libmbfl/filters/mbfilter_htmlent.c?r1=1.7&r2=1.8)

\* CONFIRM:

<http://www.php.net/ChangeLog-5.php#5.2.7>

\* CONFIRM:

<http://wiki.rpath.com/Advisories:rPSA-2009-0035>

\* CONFIRM:

<http://support.apple.com/kb/HT3549>

\* APPLE: APPLE-SA-2009-05-12

<http://lists.apple.com/archives/security-announce/2009/May/msg00002.html>

\* DEBIAN: DSA-1789

<http://www.debian.org/security/2009/dsa-1789>

\* FEDORA: FEDORA-2009-3768

<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01451.html>

\* FEDORA: FEDORA-2009-3848

<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01465.html>

\* HP: HPSBUX02431

<http://marc.info/?l=bugtraq&m=124654546101607&w=2>

\* HP: HPSBUX02465

<http://marc.info/?l=bugtraq&m=125631037611762&w=2>

\* MANDRIVA: MDVSA-2009:045

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:045>

\* REDHAT: RHSA-2009:0350

<http://www.redhat.com/support/errata/RHSA-2009-0350.html>

\* SUSE: SUSE-SR:2009:004

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

\* SUSE: SUSE-SR:2009:008

<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00003.html>

\* CERT: TA09-133A

<http://www.us-cert.gov/cas/techalerts/TA09-133A.html>

\* BID: 32948  
<http://www.securityfocus.com/bid/32948>  
\* SECTRACK: 1021482  
<http://securitytracker.com/id?1021482>  
\* SECUNIA: 34642  
<http://secunia.com/advisories/34642>  
\* SECUNIA: 35003  
<http://secunia.com/advisories/35003>  
\* SECUNIA: 35074  
<http://secunia.com/advisories/35074>  
\* SECUNIA: 35306  
<http://secunia.com/advisories/35306>  
\* SECUNIA: 35650  
<http://secunia.com/advisories/35650>  
\* VUPEN: ADV-2009-1297  
<http://www.vupen.com/english/advisories/2009/1297>  
\* XF: php-multibyte-bo(47525)  
<http://xforce.iss.net/xforce/xfdb/47525>

#### CVE Reference:

CVE-2008-5557 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18645 PHP `php_getuid` safe mode restrictions bypass Vulnerability

PHP 5 before 5.2.7 does not properly initialize the `page_uid` and `page_gid` global variables for use by the SAPI `php_getuid` function, which allows context-dependent attackers to bypass `safe_mode` restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of `/etc` for the `error_log` variable.

The issue has been fixed in PHP version 5.2.7.

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

#### References:

\* SREASONRES: 20081205 PHP 5.2.6 SAPI `php_getuid()` overload  
[http://securityreason.com/achievement\\_securityalert/59](http://securityreason.com/achievement_securityalert/59)  
\* BUGTRAQ: 20081206 SecurityReason: PHP 5.2.6 SAPI `php_getuid()` overload  
<http://www.securityfocus.com/archive/1/archive/1/498985/100/0/threaded>  
\* BUGTRAQ: 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl  
<http://www.securityfocus.com/archive/1/archive/1/501376/100/0/threaded>  
\* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.2.7>  
\* CONFIRM:  
<http://wiki.rpath.com/Advisories:rPSA-2009-0035>  
\* DEBIAN: DSA-1789  
<http://www.debian.org/security/2009/dsa-1789>  
\* HP: HPSBUX02431  
<http://marc.info/?l=bugtraq&m=124654546101607&w=2>  
\* HP: HPSBUX02465  
<http://marc.info/?l=bugtraq&m=125631037611762&w=2>  
\* MANDRIVA: MDVSA-2009:045  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:045>  
\* BID: 32688  
<http://www.securityfocus.com/bid/32688>  
\* OSVDB: 52207  
<http://osvdb.org/52207>  
\* OSVDB: 50483  
<http://osvdb.org/50483>  
\* SECUNIA: 35003  
<http://secunia.com/advisories/35003>  
\* SECUNIA: 35650  
<http://secunia.com/advisories/35650>  
\* XF: php-getuid-safemode-bypass(47318)  
<http://xforce.iss.net/xforce/xfdb/47318>

#### CVE Reference:

CVE-2008-5624 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## • 18646 PHP error\_log Safe Mode Restriction-Bypass Vulnerability

PHP 5 before 5.2.7 does not enforce the error\_log safe\_mode restrictions when safe\_mode is enabled through a php\_admin\_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php\_value error\_log" entry in a .htaccess file.

The issue has been fixed in PHP version 5.2.7.

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

### References:

- \* SREASONRES: 20081120 PHP 5.2.6 (error\_log) safe\_mode bypass  
[http://securityreason.com/achievement\\_securityalert/57](http://securityreason.com/achievement_securityalert/57)
- \* BUGTRAQ: 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl  
<http://www.securityfocus.com/archive/1/archive/1/501376/100/0/threaded>
- \* BUGTRAQ: 20081120 SecurityReason : PHP 5.2.6 (error\_log) safe\_mode bypass  
<http://archives.neohapsis.com/archives/bugtraq/2008-11/0152.html>
- \* MILWORM: 7171  
<http://www.milw0rm.com/exploits/7171>
- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.2.7>
- \* CONFIRM:  
<http://wiki.rpath.com/Advisories:rPSA-2009-0035>
- \* HP: HPSBUX02431  
<http://marc.info/?l=bugtraq&m=124654546101607&w=2>
- \* HP: HPSBUX02465  
<http://marc.info/?l=bugtraq&m=125631037611762&w=2>
- \* MANDRIVA: MDVSA-2009:045  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:045>
- \* BID: 32383  
<http://www.securityfocus.com/bid/32383>
- \* OSVDB: 52205  
<http://osvdb.org/52205>
- \* SECUNIA: 35650  
<http://secunia.com/advisories/35650>
- \* XF: php-error-safemode-bypass(47314)  
<http://xforce.iss.net/xforce/xfdb/47314>

### CVE Reference:

CVE-2008-5625 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## • 18647 PHP ZipArchive::extractTo() '.zip' Files Directory Traversal Vulnerability

Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.

The issue has been fixed in PHP version 5.2.7.

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

### References:

- \* BUGTRAQ: 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl  
<http://www.securityfocus.com/archive/1/archive/1/501376/100/0/threaded>
- \* BUGTRAQ: 20081204 Advisory 06/2008: PHP ZipArchive::extractTo() Directory Traversal Vulnerability  
<http://archives.neohapsis.com/archives/bugtraq/2008-12/0039.html>
- \* MLIST: [oss-security] 20081204 CVE for SE-2008-06 in PHP 5.2.7 (ZipArchive)  
<http://www.openwall.com/lists/oss-security/2008/12/04/3>
- \* MISC:  
<http://www.sektioneins.de/advisories/SE-2008-06.txt>
- \* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.2.7>
- \* CONFIRM:  
<http://wiki.rpath.com/Advisories:rPSA-2009-0035>
- \* DEBIAN: DSA-1789  
<http://www.debian.org/security/2009/dsa-1789>

\* FEDORA: FEDORA-2009-3768  
<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01451.html>  
\* FEDORA: FEDORA-2009-3848  
<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg01465.html>  
\* HP: HPSBUX02431  
<http://marc.info/?l=bugtraq&m=124654546101607&w=2>  
\* HP: HPSBUX02465  
<http://marc.info/?l=bugtraq&m=125631037611762&w=2>  
\* MANDRIVA: MDVSA-2009:045  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:045>  
\* REDHAT: RHSA-2009:0350  
<http://www.redhat.com/support/errata/RHSA-2009-0350.html>  
\* SUSE: SUSE-SR:2009:004  
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>  
\* BID: 32625  
<http://www.securityfocus.com/bid/32625>  
\* OSVDB: 50480  
<http://osvdb.org/50480>  
\* SECTRACK: 1021303  
<http://www.securitytracker.com/id?1021303>  
\* SECUNIA: 35003  
<http://secunia.com/advisories/35003>  
\* SECUNIA: 35306  
<http://secunia.com/advisories/35306>  
\* SECUNIA: 35650  
<http://secunia.com/advisories/35650>  
\* XF: php-ziparchive-directory-traversal(47079)  
<http://xforce.iss.net/xforce/xfdb/47079>

#### CVE Reference:

CVE-2008-5658 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18648 PHP magic\_quotes\_gpc Security Bypass Weakness

PHP 5.2.7 contains an incorrect change to the FILTER\_UNSAFE\_RAW functionality, and unintentionally disables magic\_quotes\_gpc regardless of the actual magic\_quotes\_gpc setting, which might make it easier for context-dependent attackers to conduct SQL injection attacks and unspecified other attacks.

The issue has been fixed in PHP version 5.2.8.

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

#### References:

\* CONFIRM:  
<http://bugs.php.net/bug.php?id=42718>  
\* CONFIRM:  
<http://www.php.net/ChangeLog-5.php#5.2.8>  
\* CONFIRM:  
<http://www.php.net/archive/2008.php#id2008-12-07-1>  
\* CONFIRM:  
<http://www.php.net/archive/2008.php#id2008-12-08-1>  
\* CONFIRM:  
<http://bugs.php.net/bug.php?id=46759>  
\* BID: 32673  
<http://www.securityfocus.com/bid/32673>  
\* SECTRACK: 1021393  
<http://www.securitytracker.com/id?1021393>

#### CVE Reference:

CVE-2008-5844 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18649 OpenSSL Network Security Services (NSS) library certificate spoofing Vulnerability

The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.

Users of OpenSSL 0.9.8 on affected platforms should update to 0.9.8l which contains a patch to correct this issue.

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

#### References:

- \* CONFIRM:  
[https://bugzilla.redhat.com/show\\_bug.cgi?id=CVE-2009-2409](https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2009-2409)
- \* CONFIRM:  
<http://java.sun.com/j2se/1.5.0/ReleaseNotes.html>
- \* CONFIRM:  
<http://java.sun.com/javase/6/webnotes/6u17.html>
- \* CONFIRM:  
<http://support.apple.com/kb/HT3937>
- \* APPLE: APPLE-SA-2009-11-09-1  
<http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>
- \* DEBIAN: DSA-1888  
<http://lists.debian.org/debian-security-announce/2009/msg00209.html>
- \* DEBIAN: DSA-1874  
<http://www.debian.org/security/2009/dsa-1874>
- \* GENTOO: GLSA-200911-02  
<http://security.gentoo.org/glsa/glsa-200911-02.xml>
- \* GENTOO: GLSA-200912-01  
<http://security.gentoo.org/glsa/glsa-200912-01.xml>
- \* MANDRIVA: MDVSA-2009:197  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:197>
- \* MANDRIVA: MDVSA-2009:216  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:216>
- \* MANDRIVA: MDVSA-2009:258  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:258>
- \* REDHAT: RHSA-2009:1207  
<http://www.redhat.com/support/errata/RHSA-2009-1207.html>
- \* REDHAT: RHSA-2009:1432  
<http://www.redhat.com/support/errata/RHSA-2009-1432.html>
- \* UBUNTU: USN-810-1  
<http://www.ubuntu.com/usn/usn-810-1>
- \* UBUNTU: USN-810-2  
<http://www.ubuntu.com/support/documentation/usn/usn-810-2>
- \* SECTRACK: 1022631  
<http://www.securitytracker.com/id?1022631>
- \* SECUNIA: 36139  
<http://secunia.com/advisories/36139>
- \* SECUNIA: 36157  
<http://secunia.com/advisories/36157>
- \* SECUNIA: 36739  
<http://secunia.com/advisories/36739>
- \* SECUNIA: 36434  
<http://secunia.com/advisories/36434>
- \* SECUNIA: 37386  
<http://secunia.com/advisories/37386>
- \* VUPEN: ADV-2009-2085  
<http://www.vupen.com/english/advisories/2009/2085>
- \* VUPEN: ADV-2009-3184  
<http://www.vupen.com/english/advisories/2009/3184>

#### CVE Reference:

CVE-2009-2409 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2009-4484 MySQL CVSS 2.0 Score = 7.5

Buffer overflow in the server in MySQL 5.0.51a on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by the vd\_mysql5 module in VulnDisco Pack Professional 8.11. NOTE: as of 20091229, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.

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

#### References:

MISC: <http://www.intevydis.com/blog/?p=57>

**CVE Reference:** [CVE-2009-4484](#)

• **CVE-2009-4361 IBM CVSS 2.0 Score = 7.2**

Multiple buffer overflows in qoslist in IBM AIX 6.1 allow local users to cause a denial of service (application crash) or possibly gain privileges via a long string argument. NOTE: some of these details are obtained from third party information.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2009/3600>

BID: <http://www.securityfocus.com/bid/37413>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ66966>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ66917>

SECUNIA: <http://secunia.com/advisories/37833>

**CVE Reference:** [CVE-2009-4361](#)

• **CVE-2009-4362 IBM CVSS 2.0 Score = 7.2**

Multiple buffer overflows in qosmod in IBM AIX 6.1 allow local users to cause a denial of service (application crash) or possibly gain privileges via long string arguments. NOTE: some of these details are obtained from third party information.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2009/3600>

BID: <http://www.securityfocus.com/bid/37412>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ66967>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ66918>

SECUNIA: <http://secunia.com/advisories/37833>

**CVE Reference:** [CVE-2009-4362](#)

• **CVE-2009-4143 PHP CVSS 2.0 Score = 7.5**

PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save\_path directive.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2009/3593>

BID: <http://www.securityfocus.com/bid/37390>

CONFIRM: [http://www.php.net/releases/5\\_2\\_12.php](http://www.php.net/releases/5_2_12.php)

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

SECUNIA: <http://secunia.com/advisories/37821>

**CVE Reference:** [CVE-2009-4143](#)

• **CVE-2009-4418 PHP CVSS 2.0 Score = 5.0**

The unserialize function in PHP 5.3.0 and earlier allows context-dependent attackers to cause a denial of service (resource consumption) via a deeply nested serialized variable, as demonstrated by a string beginning with a:1: followed by many {a:1: sequences.

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

**References:**

MISC: <http://www.suspekt.org/downloads/POC2009-ShockingNewsInPHPExploitation.pdf>

MISC: <http://www.suspekt.org/2009/11/28/shocking-news-in-php-exploitation/>

**CVE Reference:** [CVE-2009-4418](#)

• **CVE-2009-4142 PHP CVSS 2.0 Score = 4.3**

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.

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

**References:**

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

VUPEN: <http://www.vupen.com/english/advisories/2009/3593>

BID: <http://www.securityfocus.com/bid/37389>

CONFIRM: [http://www.php.net/releases/5\\_2\\_12.php](http://www.php.net/releases/5_2_12.php)

SECTRACK: <http://securitytracker.com/id?1023372>

SECUNIA: <http://secunia.com/advisories/37821>

CONFIRM: <http://bugs.php.net/bug.php?id=49785>

**CVE Reference:** [CVE-2009-4142](#)

• **CVE-2009-3792 Adobe CVSS 2.0 Score = 10.0**

Directory traversal vulnerability in Adobe Flash Media Server (FMS) before 3.5.3 allows attackers to load arbitrary DLL files via unspecified vectors.

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

**References:**

BID: <http://www.securityfocus.com/bid/37420>

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb09-18.html>

**CVE Reference:** [CVE-2009-3792](#)

• **CVE-2009-3791 Adobe CVSS 2.0 Score = 5.0**

Unspecified vulnerability in Adobe Flash Media Server (FMS) before 3.5.3 allows attackers to cause a denial of service (resource exhaustion) via unknown vectors.

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

**References:**

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb09-18.html>

BID: <http://www.securityfocus.com/bid/37419>

**CVE Reference:** [CVE-2009-3791](#)

**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)