

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

[Nimda Worm Scanner](#) - The S4 Nimda Worm 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 MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=nimdawormscanner>

This Week in Review

The fed sued for social-network surveillance. SSL products not so safe. Microsoft fixes IE hole. Be very careful - IRS does not send out emails.

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

• EFF sues feds for info on social-network surveillance

The Electronic Frontier Foundation sued the CIA, the U.S. Department of Defense, Department of Justice, and three other government agencies on Tuesday for allegedly refusing to release information about how they are using social networks in surveillance and investigations.

The nonprofit Internet rights watchdog group formally asked more than a dozen agencies or departments in early October to provide records about federal guidelines on the use of sites like Facebook, Twitter, and Flickr for investigative or data gathering purposes, according to the lawsuit. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10407224-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Clientless SSL VPN products vulnerable, says US-CERT

US-CERT this week warned of a vulnerability that impacts a host of clientless SSL VPN products and could lead to bypassed authentication and other internet attacks.

Clientless SSL products provide web-based access to intranet sites, internal file shares and remote desktops, without needing to install a traditional VPN client.

Many of these products operate in a way that bypasses fundamental web browser domain-based security mechanisms, US-CERT said. Products from Cisco, Citrix, McAfee, Intel and a number of other vendors are affected.
SC Magazine

Full Story :

http://www.scmagazineus.com/clientless-ssl-vpn-products-vulnerable-says-us-cert/article/159037/?utm_source=feed

• Microsoft to plug critical IE hole targeted by exploit code

Microsoft said on Thursday that it will offer six updates for 12 vulnerabilities next week including a critical hole in Internet Explorer that affects Windows 7 and other current versions of the operating system for which exploit code has been released.

Late last month, Microsoft said it was investigating an IE vulnerability after someone released proof-of-concept code affecting IE 6 and IE 7 that could be used to take control of computers.

Microsoft described the problem in an advisory issued November 23: "The vulnerability exists as an invalid pointer reference of Internet Explorer. It is possible under certain conditions for a CSS/Style object to be accessed after the object is deleted. In a specially-crafted attack, Internet Explorer attempting to access a freed object can lead to running attacker-supplied code." Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10408898-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Zeus spreading through drive-by download

The notorious information-stealing Zeus trojan is currently spreading via drive-by download, said security researchers at IT management software and solutions vendor CA.

Those behind Zeus, or Zbot, recently began circulating spam claiming to come from the Internal Revenue Service (IRS), requesting users submit a "tax refund request form" by clicking on a link that is provided.

Clicking takes victims to a website that attempts to perform a drive-by download, meaning users do not need to take any further action to be infected, Don DeBolt, director of threat research at CA, told SCMagazineUS.com on Monday.
SC Magazine

Full Story :

http://www.scmagazineus.com/zeus-spreading-through-drive-by-download/article/158691/?utm_source=feedburner&

• Cameroon, China riskiest country domains, McAfee finds

Websites registered in the African nation of Cameroon are the most likely domains to infect users' computers with malware, according to McAfee's annual study on the web's riskiest recesses.

The report, released Wednesday, found that nearly 37 percent of websites ending in .cm posed a security threat. According to McAfee, criminals known as typosquatters are taking advantage of the domain extension's spelling similarity to the popular .com, in hopes users mistype the URL they actually want to reach and instead surf to sites pushing malware.

Researchers studied some 27 million websites as part of their analysis and determined that 5.8 percent, or roughly 1.5 million, pose a risk. SC Magazine

Full Story :

http://www.scmagazineus.com/cameroon-china-riskiest-country-domains-mcafee-finds/article/158944/?utm_source=feedburner&

New Vulnerabilities Tested in SecureScout

• 18610 Apache Tomcat Information Disclosure Vulnerability (CVE-2008-5515)

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

When using a RequestDispatcher obtained from the Request, the target path was normalized before the query string was removed. A request that included a specially crafted request parameter could be used to access content that would otherwise be protected by a security constraint or by locating it in under the WEB-INF directory.

The issue has been addressed in Apache Tomcat version 6.0.19, 5.5.28, and 4.1.40.

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

References:

- * BUGTRAQ: 20090608 [SECURITY] CVE-2008-5515 RequestDispatcher directory traversal vulnerability
<http://www.securityfocus.com/archive/1/archive/1/504170/100/0/threaded>
- * BUGTRAQ: 20090610 [SECURITY] UPDATED CVE-2008-5515 RequestDispatcher directory traversal vulnerability
<http://www.securityfocus.com/archive/1/archive/1/504202/100/0/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.fujitsu.com/global/support/software/security/products-f/interstage-200902e.html>
- * CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2009-0016.html>
- * FEDORA: FEDORA-2009-11352
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01216.html>
- * FEDORA: FEDORA-2009-11356
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01246.html>
- * FEDORA: FEDORA-2009-11374
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01156.html>
- * MANDRIVA: MDVSA-2009:136
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:136>
- * MANDRIVA: MDVSA-2009:138
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:138>
- * SUNALERT: 263529
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-263529-1>
- * SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
- * JVN: JVN#63832775
<http://jvn.jp/en/jp/JVN63832775/index.html>
- * BID: 35263
<http://www.securityfocus.com/bid/35263>
- * SECUNIA: 35393
<http://secunia.com/advisories/35393>
- * SECUNIA: 35685
<http://secunia.com/advisories/35685>
- * SECUNIA: 35788
<http://secunia.com/advisories/35788>
- * SECUNIA: 37460
<http://secunia.com/advisories/37460>
- * VUPEN: ADV-2009-1520
<http://www.vupen.com/english/advisories/2009/1520>
- * VUPEN: ADV-2009-1535
<http://www.vupen.com/english/advisories/2009/1535>
- * VUPEN: ADV-2009-1856
<http://www.vupen.com/english/advisories/2009/1856>
- * VUPEN: ADV-2009-3316
<http://www.vupen.com/english/advisories/2009/3316>

CVE Reference:

CVE-2008-5515 (cve.mitre.org, nvd.nist.gov)

● 18611 Apache Tomcat Insecure default password Vulnerability (CVE-2009-3548)

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

The Windows installer defaults to a blank password for the administrative user. If this is not changed during the install process, then by default a user is created with the name admin, roles admin and manager and a blank password.

The issue has been addressed in Apache Tomcat version 6.0.21, 5.5.29.

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

References:

- * BUGTRAQ: 20091109 [SECURITY] CVE-2009-3548 Apache Tomcat Windows Installer insecure default administrative password
<http://www.securityfocus.com/archive/1/archive/1/507720/100/0/threaded>
- * MISC:
<http://markmail.org/thread/wfu4nff5chvkb6xp>
- * CONFIRM:
<http://tomcat.apache.org/security-5.html>
- * CONFIRM:
<http://tomcat.apache.org/security-6.html>
- * BID: 36954
<http://www.securityfocus.com/bid/36954>
- * SECTRACK: 1023146
<http://www.securitytracker.com/id?1023146>
- * VUPEN: ADV-2009-3185
<http://www.vupen.com/english/advisories/2009/3185>
- * XF: tomcat-admin-default-password(54182)
<http://xforce.iss.net/xforce/xfdb/54182>

CVE Reference:

CVE-2009-3548 (cve.mitre.org, nvd.nist.gov)

• 18612 Apache Tomcat Denial of Service Vulnerability (CVE-2009-0033)

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

If Tomcat receives a request with invalid headers via the Java AJP connector, it does not return an error and instead closes the AJP connection. In case this connector is member of a mod_jk load balancing worker, this member will be put into an error state and will be blocked from use for approximately one minute. The behavior can be used for a denial of service attack using a carefully crafted request.

The issue has been addressed in Apache Tomcat version 6.0.19, 5.5.28, and 4.1.40.

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

References:

- * BUGTRAQ: 20090603 [SECURITY] CVE-2009-0033 Apache Tomcat DoS when using Java AJP connector
<http://www.securityfocus.com/archive/1/archive/1/504044/100/0/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://svn.apache.org/viewvc?rev=742915&view=rev>
- * CONFIRM:
<http://svn.apache.org/viewvc?rev=781362&view=rev>
- * 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-2009-0016.html>
- * FEDORA: FEDORA-2009-11352
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01216.html>
- * FEDORA: FEDORA-2009-11356
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01246.html>
- * FEDORA: FEDORA-2009-11374
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01156.html>
- * MANDRIVA: MDVSA-2009:136
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:136>
- * MANDRIVA: MDVSA-2009:138
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:138>
- * SUNALERT: 263529
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-263529-1>

* SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
* JVN: JVN#87272440
<http://jvn.jp/en/jp/JVN87272440/index.html>
* BID: 35193
<http://www.securityfocus.com/bid/35193>
* SECTRACK: 1022331
<http://securitytracker.com/id?1022331>
* SECUNIA: 35326
<http://secunia.com/advisories/35326>
* SECUNIA: 35344
<http://secunia.com/advisories/35344>
* SECUNIA: 35685
<http://secunia.com/advisories/35685>
* SECUNIA: 35788
<http://secunia.com/advisories/35788>
* SECUNIA: 37460
<http://secunia.com/advisories/37460>
* VUPEN: ADV-2009-1496
<http://www.vupen.com/english/advisories/2009/1496>
* VUPEN: ADV-2009-1856
<http://www.vupen.com/english/advisories/2009/1856>
* VUPEN: ADV-2009-3316
<http://www.vupen.com/english/advisories/2009/3316>
* XF: tomcat-ajp-dos(50928)
<http://xforce.iss.net/xforce/xfdb/50928>

CVE Reference:

CVE-2009-0033 (cve.mitre.org, nvd.nist.gov)

• 18613 Apache Tomcat Information disclosure Vulnerability (CVE-2009-0580)

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

Due to insufficient error checking in some authentication classes, Tomcat allows for the enumeration (brute force testing) of user names by supplying illegally URL encoded passwords. The attack is possible if FORM based authentication (`j_security_check`) is used with the MemoryRealm.

The issue has been addressed in Apache Tomcat version 6.0.19, 5.5.28, and 4.1.40.

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

References:

* BUGTRAQ: 20090603 [SECURITY] CVE-2009-0580 Apache Tomcat User enumeration vulnerability with FORM authentication
<http://www.securityfocus.com/archive/1/archive/1/504045/100/0/threaded>
* BUGTRAQ: 20090604 Re: [SECURITY] CVE-2009-0580 Apache Tomcat User enumeration vulnerability with FORM authentication
<http://www.securityfocus.com/archive/1/archive/1/504108/100/0/threaded>
* BUGTRAQ: 20090605 [SECURITY] CVE-2009-0580 UPDATED Apache Tomcat User enumeration vulnerability with FORM authentication
<http://www.securityfocus.com/archive/1/archive/1/504125/100/0/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://svn.apache.org/viewvc?rev=747840&view=rev>
* CONFIRM:
<http://svn.apache.org/viewvc?rev=781379&view=rev>
* CONFIRM:
<http://svn.apache.org/viewvc?rev=781382&view=rev>
* 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-2009-0016.html>

* FEDORA: FEDORA-2009-11352
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01216.html>

* FEDORA: FEDORA-2009-11356
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01246.html>

* FEDORA: FEDORA-2009-11374
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01156.html>

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

* MANDRIVA: MDVSA-2009:138
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:138>

* SUNALERT: 263529
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-263529-1>

* SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>

* BID: 35196
<http://www.securityfocus.com/bid/35196>

* SECTRACK: 1022332
<http://securitytracker.com/id?1022332>

* SECUNIA: 35326
<http://secunia.com/advisories/35326>

* SECUNIA: 35344
<http://secunia.com/advisories/35344>

* SECUNIA: 35685
<http://secunia.com/advisories/35685>

* SECUNIA: 35788
<http://secunia.com/advisories/35788>

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

* VUPEN: ADV-2009-1496
<http://www.vupen.com/english/advisories/2009/1496>

* VUPEN: ADV-2009-1856
<http://www.vupen.com/english/advisories/2009/1856>

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

* XF: tomcat-jsecuritycheck-info-disclosure(50930)
<http://xforce.iss.net/xforce/xfdb/50930>

CVE Reference:

CVE-2009-0580 (cve.mitre.org, nvd.nist.gov)

• 18614 Apache Tomcat Cross-site scripting Vulnerability (CVE-2009-0781)

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

The calendar application in the examples web application contains an XSS flaw due to invalid HTML which renders the XSS filtering protection ineffective.

The issue has been addressed in Apache Tomcat version 6.0.19, 5.5.28, and 4.1.40.

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

References:

* BUGTRAQ: 20090306 [SECURITY] CVE-2009-0781 XSS in Apache Tomcat examples web application
<http://www.securityfocus.com/archive/1/archive/1/501538/100/0/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-2009-0016.html>

* FEDORA: FEDORA-2009-11352
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01216.html>

* FEDORA: FEDORA-2009-11356
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01246.html>

* FEDORA: FEDORA-2009-11374
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01156.html>
* MANDRIVA: MDVSA-2009:136
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:136>
* MANDRIVA: MDVSA-2009:138
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:138>
* SUNALERT: 263529
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-263529-1>
* SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
* SECUNIA: 35685
<http://secunia.com/advisories/35685>
* SECUNIA: 35788
<http://secunia.com/advisories/35788>
* SECUNIA: 37460
<http://secunia.com/advisories/37460>
* VUPEN: ADV-2009-1856
<http://www.vupen.com/english/advisories/2009/1856>
* VUPEN: ADV-2009-3316
<http://www.vupen.com/english/advisories/2009/3316>
* XF: tomcat-cal2-xss(49213)
<http://xforce.iss.net/xforce/xfdb/49213>

CVE Reference:

CVE-2009-0781 (cve.mitre.org, nvd.nist.gov)

● 18615 Apache Tomcat Information disclosure Vulnerability (CVE-2009-0783)

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

Bugs 29936 and 45933 allowed a web application to replace the XML parser used by Tomcat to process web.xml, context.xml and tld files. In limited circumstances these bugs may allow a rogue web application to view and/or alter the web.xml, context.xml and tld files of other web applications deployed on the Tomcat instance.

The issue has been addressed in Apache Tomcat version 6.0.19, 5.5.28, and 4.1.40.

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

References:

* BUGTRAQ: 20090604 [SECURITY] CVE-2009-0783 Apache Tomcat Information disclosure
<http://www.securityfocus.com/archive/1/archive/1/504090/100/0/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://svn.apache.org/viewvc?rev=652592&view=rev>
* CONFIRM:
<http://svn.apache.org/viewvc?rev=681156&view=rev>
* CONFIRM:
<http://svn.apache.org/viewvc?rev=739522&view=rev>
* CONFIRM:
<http://svn.apache.org/viewvc?rev=781542&view=rev>
* CONFIRM:
<http://svn.apache.org/viewvc?rev=781708&view=rev>
* 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:
https://issues.apache.org/bugzilla/show_bug.cgi?id=29936
* CONFIRM:
https://issues.apache.org/bugzilla/show_bug.cgi?id=45933
* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2009-0016.html>
* FEDORA: FEDORA-2009-11352
<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01216.html>
* FEDORA: FEDORA-2009-11356

<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01246.html>

* FEDORA: FEDORA-2009-11374

<https://www.redhat.com/archives/fedora-package-announce/2009-November/msg01156.html>

* MANDRIVA: MDVSA-2009:136

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

* MANDRIVA: MDVSA-2009:138

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:138>

* SUNALERT: 263529

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-263529-1>

* SUSE: SUSE-SR:2009:012

<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>

* BID: 35416

<http://www.securityfocus.com/bid/35416>

* SECTRAK: 1022336

<http://www.securitytracker.com/id?1022336>

* SECUNIA: 35685

<http://secunia.com/advisories/35685>

* SECUNIA: 35788

<http://secunia.com/advisories/35788>

* SECUNIA: 37460

<http://secunia.com/advisories/37460>

* VUPEN: ADV-2009-1856

<http://www.vupen.com/english/advisories/2009/1856>

* VUPEN: ADV-2009-3316

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

* XF: tomcat-xml-information-disclosure(51195)

<http://xforce.iss.net/xforce/xfdb/51195>

CVE Reference:

CVE-2009-0783 (cve.mitre.org, nvd.nist.gov)

• 18616 Apache Tomcat Cross-site scripting Vulnerability (CVE-2008-1232)

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

The message argument of `HttpServletResponse.sendError()` call is not only displayed on the error page, but is also used for the reason-phrase of HTTP response. This may include characters that are illegal in HTTP headers. It is possible for a specially crafted message to result in arbitrary content being injected into the HTTP response. For a successful XSS attack, unfiltered user supplied data must be included in the message argument.

The issue has been addressed in Apache Tomcat version 6.0.17, 5.5.27, and 4.1.38.

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

References:

* BUGTRAQ: 20080801 [CVE-2008-1232] Apache Tomcat XSS vulnerability

<http://www.securityfocus.com/archive/1/archive/1/495021/100/0/threaded>

* BUGTRAQ: 20090616 CA20090615-02: CA Service Desk Tomcat Cross Site Scripting Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/504351/100/0/threaded>

* BUGTRAQ: 20090806 CA20090806-02: Security Notice for Unicenter Asset Portfolio Management, Unicenter Desktop and Server Management, Unicenter Patch Management

<http://www.securityfocus.com/archive/1/archive/1/505556/100/0/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://support.apple.com/kb/HT3216>

* CONFIRM:

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

* CONFIRM:

<http://www.vmware.com/security/advisories/VMSA-2009-0002.html>

* CONFIRM:

<http://community.ca.com/blogs/casecurityresponseblog/archive/2009/06/15/ca20090615-02-ca-service-desk-tomcat-cross>

* CONFIRM:
<http://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=209500>

* CONFIRM:
<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=209500>

* CONFIRM:
<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=214095>

* 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-2008-8113
<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00859.html>

* FEDORA: FEDORA-2008-8130
<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00889.html>

* FEDORA: FEDORA-2008-7977
<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00712.html>

* HP: HPSBUX02401
<http://marc.info/?l=bugtraq&w=2&m=123376588623823&w=2>

* MANDRIVA: MDVSA-2008:188
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:188>

* REDHAT: RHSA-2008:0648
<http://www.redhat.com/support/errata/RHSA-2008-0648.html>

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

* REDHAT: RHSA-2008:0864
<http://www.redhat.com/support/errata/RHSA-2008-0864.html>

* SUSE: SUSE-SR:2008:018
<http://lists.opensuse.org/opensuse-security-announce/2008-09/msg00004.html>

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

* BID: 30496
<http://www.securityfocus.com/bid/30496>

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

* OVAL: oval:org.mitre.oval:def:5985
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5985>

* SECUNIA: 33999
<http://secunia.com/advisories/33999>

* SECUNIA: 34013
<http://secunia.com/advisories/34013>

* SECUNIA: 35474
<http://secunia.com/advisories/35474>

* SECUNIA: 36108
<http://secunia.com/advisories/36108>

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

* VUPEN: ADV-2008-2305
<http://www.frsirt.com/english/advisories/2008/2305>

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

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

* VUPEN: ADV-2009-0320
<http://www.frsirt.com/english/advisories/2009/0320>

* SECTRACK: 1020622
<http://www.securitytracker.com/id?1020622>

* SECUNIA: 31379
<http://secunia.com/advisories/31379>

* SECUNIA: 31381
<http://secunia.com/advisories/31381>

* SECUNIA: 31639
<http://secunia.com/advisories/31639>

* SECUNIA: 31891
<http://secunia.com/advisories/31891>

* SECUNIA: 31865
<http://secunia.com/advisories/31865>

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

* SECUNIA: 31982

<http://secunia.com/advisories/31982>

* SECUNIA: 33797

<http://secunia.com/advisories/33797>

* SECUNIA: 32120

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

* SECUNIA: 32266

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

* SREASON: 4098

<http://securityreason.com/securityalert/4098>

* VUPEN: ADV-2009-0503

<http://www.vupen.com/english/advisories/2009/0503>

* VUPEN: ADV-2009-1609

<http://www.vupen.com/english/advisories/2009/1609>

* VUPEN: ADV-2009-2194

<http://www.vupen.com/english/advisories/2009/2194>

* VUPEN: ADV-2009-3316

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

* XF: tomcat-httpservletresponse-xss(44155)

<http://xforce.iss.net/xforce/xfdb/44155>

CVE Reference:

CVE-2008-1232 (cve.mitre.org, nvd.nist.gov)

• 18617 Apache Tomcat Cross-site scripting Vulnerability (CVE-2008-1947)

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

The Host Manager web application did not escape user provided data before including it in the output. This enabled a XSS attack. This application now filters 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 has been addressed in Apache Tomcat version 6.0.17, 5.5.27.

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

References:

* BUGTRAQ: 20080602 [SECURITY] CVE-2008-1947: Tomcat host-manager XSS vulnerability

<http://www.securityfocus.com/archive/1/archive/1/492958/100/0/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>

* MLIST: [tomcat-user] 20080602 [SECURITY] CVE-2008-1947: Tomcat host-manager XSS vulnerability

<http://marc.info/?l=tomcat-user&m=121244319501278&w=2>

* CONFIRM:

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

* CONFIRM:

<http://tomcat.apache.org/security-6.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-2009-0002.html>

* 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-1593

<http://www.debian.org/security/2008/dsa-1593>

* FEDORA: FEDORA-2008-8113

<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00859.html>

* FEDORA: FEDORA-2008-8130

<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00889.html>

* FEDORA: FEDORA-2008-7977

<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00712.html>

* HP: HPSBUX02401

<http://marc.info/?l=bugtraq&m=123376588623823&w=2>

* MANDRIVA: MDVSA-2008:188

<http://www.mandriva.com/security/advisories?name=MDVSA-2008:188>

* REDHAT: RHSA-2008:0648
<http://www.redhat.com/support/errata/RHSA-2008-0648.html>

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

* REDHAT: RHSA-2008:0864
<http://www.redhat.com/support/errata/RHSA-2008-0864.html>

* SUSE: SUSE-SR:2008:014
<http://lists.opensuse.org/opensuse-security-announce/2008-07/msg00001.html>

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

* BID: 29502
<http://www.securityfocus.com/bid/29502>

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

* OVAL: oval:org.mitre.oval:def:6009
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6009>

* SECUNIA: 33999
<http://secunia.com/advisories/33999>

* SECUNIA: 34013
<http://secunia.com/advisories/34013>

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

* VUPEN: ADV-2008-1725
<http://www.frsirt.com/english/advisories/2008/1725>

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

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

* VUPEN: ADV-2009-0320
<http://www.frsirt.com/english/advisories/2009/0320>

* SECTRACK: 1020624
<http://www.securitytracker.com/id?1020624>

* SECUNIA: 30500
<http://secunia.com/advisories/30500>

* SECUNIA: 30592
<http://secunia.com/advisories/30592>

* SECUNIA: 30967
<http://secunia.com/advisories/30967>

* SECUNIA: 31639
<http://secunia.com/advisories/31639>

* SECUNIA: 31891
<http://secunia.com/advisories/31891>

* SECUNIA: 31865
<http://secunia.com/advisories/31865>

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

* SECUNIA: 33797
<http://secunia.com/advisories/33797>

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

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

* VUPEN: ADV-2009-0503
<http://www.vupen.com/english/advisories/2009/0503>

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

* XF: apache-tomcat-hostmanager-xss(42816)
<http://xforce.iss.net/xforce/xfdb/42816>

CVE Reference:

CVE-2008-1947 (cve.mitre.org, nvd.nist.gov)

• 18618 Apache Tomcat Information disclosure Vulnerability (CVE-2008-2370)

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

When using a RequestDispatcher the target path was normalised before the query string was removed. A request that included a specially crafted request parameter could be used to access content that would otherwise be protected by a security constraint or by locating it in under the WEB-INF directory.

The issue has been addressed in Apache Tomcat version 6.0.17, 5.5.27, 4.1.38.

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

References:

- * BUGTRAQ: 20080801 [CVE-2008-2370] Apache Tomcat information disclosure vulnerability
<http://www.securityfocus.com/archive/1/archive/1/495022/100/0/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>
- * MLIST: [apache-announce] 20090808 [ANNOUNCE] Apache ODE 1.3.3
<http://marc.info/?l=apache-announce&m=124972618803216&w=2>
- * MLIST: [ode-user] 20090808 [ANNOUNCE] Apache ODE 1.3.3
http://mail-archives.apache.org/mod_mbox/ode-user/200908.mbox/%3Cfbdc6a970908072141w20a7a9d9ka1f896ad8073
- * 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/HT3216>
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2008-401.htm>
- * CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2009-0002.html>
- * CONFIRM:
<http://www.fujitsu.com/global/support/software/security/products-f/interstage-200902e.html>
- * 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-2008-8113
<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00859.html>
- * FEDORA: FEDORA-2008-8130
<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00889.html>
- * FEDORA: FEDORA-2008-7977
<https://www.redhat.com/archives/fedora-package-announce/2008-September/msg00712.html>
- * HP: HPSBUX02401
<http://marc.info/?l=bugtraq&m=123376588623823&w=2>
- * MANDRIVA: MDVSA-2008:188
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:188>
- * REDHAT: RHSA-2008:0648
<http://www.redhat.com/support/errata/RHSA-2008-0648.html>
- * REDHAT: RHSA-2008:0862
<http://www.redhat.com/support/errata/RHSA-2008-0862.html>
- * REDHAT: RHSA-2008:0864
<http://www.redhat.com/support/errata/RHSA-2008-0864.html>
- * SUSE: SUSE-SR:2008:018
<http://lists.opensuse.org/opensuse-security-announce/2008-09/msg00004.html>
- * SUSE: SUSE-SR:2009:004
<http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00002.html>
- * BID: 30494
<http://www.securityfocus.com/bid/30494>
- * BID: 31681
<http://www.securityfocus.com/bid/31681>
- * OVAL: oval:org.mitre.oval:def:5876
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5876>
- * SECUNIA: 33999
<http://secunia.com/advisories/33999>
- * SECUNIA: 34013
<http://secunia.com/advisories/34013>
- * SECUNIA: 35393
<http://secunia.com/advisories/35393>
- * SECUNIA: 36249
<http://secunia.com/advisories/36249>
- * SECUNIA: 37460
<http://secunia.com/advisories/37460>
- * VUPEN: ADV-2008-2305

<http://www.frsirt.com/english/advisories/2008/2305>

* VUPEN: ADV-2008-2823

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

* VUPEN: ADV-2008-2780

<http://www.frsirt.com/english/advisories/2008/2780>

* VUPEN: ADV-2009-0320

<http://www.frsirt.com/english/advisories/2009/0320>

* SECTRACK: 1020623

<http://www.securitytracker.com/id?1020623>

* SECUNIA: 31379

<http://secunia.com/advisories/31379>

* SECUNIA: 31381

<http://secunia.com/advisories/31381>

* SECUNIA: 31639

<http://secunia.com/advisories/31639>

* SECUNIA: 31891

<http://secunia.com/advisories/31891>

* SECUNIA: 31865

<http://secunia.com/advisories/31865>

* SECUNIA: 32222

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

* SECUNIA: 31982

<http://secunia.com/advisories/31982>

* SECUNIA: 33797

<http://secunia.com/advisories/33797>

* SECUNIA: 32120

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

* SECUNIA: 32266

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

* SREASON: 4099

<http://securityreason.com/securityalert/4099>

* VUPEN: ADV-2009-0503

<http://www.vupen.com/english/advisories/2009/0503>

* VUPEN: ADV-2009-1535

<http://www.vupen.com/english/advisories/2009/1535>

* VUPEN: ADV-2009-2215

<http://www.vupen.com/english/advisories/2009/2215>

* VUPEN: ADV-2009-3316

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

* XF: tomcat-requestdispatcher-info-disclosure(44156)

<http://xforce.iss.net/xforce/xfdb/44156>

CVE Reference:

CVE-2008-2370 (cve.mitre.org, nvd.nist.gov)

• 18619 Apache Tomcat Session hi-jacking Vulnerability (CVE-2008-0128)

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

When using the SingleSignOn Valve via https the Cookie JSESSIONIDSSO is transmitted without the "secure" attribute, resulting in it being transmitted to any content that is - by purpose or error - requested via http from the same server.

The issue has been addressed in Apache Tomcat version 6.0.9, 5.5.21, 4.1.38.

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

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://issues.apache.org/bugzilla/show_bug.cgi?id=41217

* CONFIRM:

<http://security-tracker.debian.net/tracker/CVE-2008-0128>

* 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-1468

<http://www.debian.org/security/2008/dsa-1468>

* 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:2008:005

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

* BID: 27365

<http://www.securityfocus.com/bid/27365>

* VUPEN: ADV-2008-0192

<http://www.frsirt.com/english/advisories/2008/0192>

* VUPEN: ADV-2009-0233

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

* SECUNIA: 28549

<http://secunia.com/advisories/28549>

* SECUNIA: 28552

<http://secunia.com/advisories/28552>

* SECUNIA: 29242

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

* SECUNIA: 31493

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

* SECUNIA: 33668

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

* XF: apache-singlesignon-information-disclosure(39804)

<http://xforce.iss.net/xforce/xfdb/39804>

CVE Reference:

CVE-2008-0128 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-3672 Microsoft CVSS 2.0 Score = 9.3

Microsoft Internet Explorer 6 and 7 allows remote attackers to execute arbitrary code via vectors involving a call to the getElementByTagName method for the CSS STYLE tag name, selection of the single element in the returned list, and a change to the outerHTML property of this element, which triggers memory corruption in the Microsoft HTML Viewer (mshtml.dll). NOTE: some of these details are obtained from third party information. NOTE: this issue was originally assigned CVE-2009-4054, but Microsoft assigned a duplicate identifier of CVE-2009-3672. CVE consumers should use this identifier instead of CVE-2009-4054.

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

References:

MISC: <http://www.symantec.com/connect/blogs/zero-day-internet-explorer-exploit-published>

BID: <http://www.securityfocus.com/bid/37085>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/507984/100/0/threaded>

CONFIRM: <http://www.microsoft.com/technet/security/advisory/977981.mspx>

CVE Reference: [CVE-2009-3672](http://cve.mitre.org/cve/2009/3672)

• CVE-2009-2686 HP CVSS 2.0 Score = 4.6

Unspecified vulnerability in HP NonStop G06.12.00 through G06.32.00, H06.08.00 through H06.18.01, and J06.04.00 through J06.07.01 allows local users to gain privileges, cause a denial of service, or obtain "access to data" via unknown vectors.

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

References:

HP: https://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01923646

HP: https://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01923646

VUPEN: <http://www.vupen.com/english/advisories/2009/3373>

SECUNIA: <http://secunia.com/advisories/37560>

CVE Reference: [CVE-2009-2686](#)

• **CVE-2009-4028 MySQL CVSS 2.0 Score = 6.4**

The `vio_verify_callback` function in `viossfactories.c` in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41, when OpenSSL is used, accepts a value of zero for the depth of X.509 certificates, which allows man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certificate, as demonstrated by a certificate presented by a server linked against the yaSSL library.

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

References:

MLIST: <http://www.openwall.com/lists/oss-security/2009/11/23/16>

MLIST: <http://www.openwall.com/lists/oss-security/2009/11/19/3>

MLIST: <http://marc.info/?l=oss-security&m=125881733826437&w=2>

MLIST: <http://lists.mysql.com/commits/87446>

CONFIRM: <http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html>

CONFIRM: <http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html>

CONFIRM: <http://bugs.mysql.com/47320>

CVE Reference: [CVE-2009-4028](#)

• **CVE-2008-7247 MySQL CVSS 2.0 Score = 6.0**

`sql/sql_table.cc` in MySQL 5.0.x through 5.0.88, 5.1.x through 5.1.41, and 6.0 before 6.0.9-alpha, when the data home directory contains a symlink to a different filesystem, allows remote authenticated users to bypass intended access restrictions by calling CREATE TABLE with a (1) DATA DIRECTORY or (2) INDEX DIRECTORY argument referring to a subdirectory that requires following this symlink.

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

References:

MLIST: <http://marc.info/?l=oss-security&m=125908040022018&w=2>

MLIST: <http://lists.mysql.com/commits/59711>

CONFIRM: <http://bugs.mysql.com/bug.php?id=39277>

CVE Reference: [CVE-2008-7247](#)

• **CVE-2009-4030 MySQL CVSS 2.0 Score = 4.4**

MySQL 5.1.x before 5.1.41 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL data home directory, related to incorrect calculation of the `mysql_unpacked_real_data_home` value. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4098 and CVE-2008-2079.

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

References:

MLIST: <http://www.openwall.com/lists/oss-security/2009/11/24/6>

MLIST: <http://www.openwall.com/lists/oss-security/2009/11/19/3>

MLIST: <http://marc.info/?l=oss-security&m=125908080222685&w=2>

MLIST: <http://marc.info/?l=oss-security&m=125908040022018&w=2>

MLIST: <http://lists.mysql.com/commits/89940>

CONFIRM: <http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html>

CONFIRM: <http://bugs.mysql.com/bug.php?id=32167>

CVE Reference: [CVE-2009-4030](#)

• **CVE-2009-4019 MySQL CVSS 2.0 Score = 4.0**

mysqld in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 does not (1) properly handle errors during execution of certain SELECT statements with subqueries, and does not (2) preserve certain null_value flags during execution of statements that use the GeomFromWKB function, which allows remote authenticated users to cause a denial of service (daemon crash) via a crafted statement.

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

References:

MLIST: <http://marc.info/?l=oss-security&m=125901161824278&w=2>

MLIST: <http://marc.info/?l=oss-security&m=125883754215621&w=2>

MLIST: <http://marc.info/?l=oss-security&m=125881733826437&w=2>

CONFIRM: <http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html>

CONFIRM: <http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html>

CONFIRM: <http://bugs.mysql.com/48291>

CONFIRM: <http://bugs.mysql.com/47780>

CVE Reference: [CVE-2009-4019](#)

• **CVE-2009-4111 Sendmail CVSS 2.0 Score = 6.8**

Argument injection vulnerability in Mail/sendmail.php in the Mail package 1.1.14, 1.2.0b2, and possibly other versions for PEAR allows remote attackers to read and write arbitrary files via a crafted \$recipients parameter, and possibly other parameters, a different vulnerability than CVE-2009-4023.

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

References:

MLIST: <http://www.openwall.com/lists/oss-security/2009/11/28/2>

MLIST: <http://www.openwall.com/lists/oss-security/2009/11/23/8>

MISC: <http://pear.php.net/bugs/bug.php?id=16200>

CVE Reference: [CVE-2009-4111](#)

• **CVE-2009-4153 IBM CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the XMLAccess component in IBM WebSphere Portal 6.1.x before 6.1.0.3 has unknown impact and attack vectors, related to the work directory.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/3367>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27014411>

BID: <http://www.securityfocus.com/bid/37159>

SECUNIA: <http://secunia.com/advisories/37526>

CVE Reference: [CVE-2009-4153](#)

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