

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

PCI compliance advice. And some advice on log management. CERT 20 years old. Financial institutions having trouble keeping hacker out.

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

• SC eConference and Expo: PCI Compliance keynote speaker shares advice

There's much controversy surrounding the Payment Card Industry Data Security Standard (DSS) mandates these days. With huge breaches of private data, like that experienced by Heartland Payment Systems (which potentially could have affected some 100 million credit cards), some are wondering just how effective PCI requirements are. Ask many experts, however, and they'll say that being compliant with PCI DSS doesn't mean your company's infrastructure is secure.

SC Magazine: What is the one area of PCI compliance that you and your peers seem to have had the most trouble with?

SC: As a professional whose company is affected by PCI mandates, in what ways do you think the PCI Security Standards Council could improve the requirements and/or guidance?

Full Story :

<http://www.scmagazineus.com/SC-eConference-and-Expo-PCI-Compliance-keynote-speaker-shares-advice/article/12>

• **Avoiding Pitfalls in Log Management Planning**

March 25, 2009 (CSO) Over the past decade cyber security has emerged as an important concern for organizations of all sizes. The increase in digitized corporate records, coupled with the rise in cyber crime, is driving organizations in the public and private sectors to invest in more protection for sensitive data and regulated or other critical assets. In just the first two months this year, the Privacy Rights Clearinghouse has noted data breaches at several financial, healthcare and educational institutions as well as federal, state and local governmental agencies.

Monitoring and Log Management

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130440&source=rss_topic1

• **Pethia: InfoSec's Challenges, Changes**

March 24, 2009 (CSO) A lot has changed in the 20 years since Rich Pethia first took the reigns as director of Carnegie Mellon University's CERT. CERT, which was initially launched as the first Internet security response organization, has evolved over the years to focus more on research and training role. Pethia, a CSO Compass Award winner, spoke with CSO about how much IT security and vulnerabilities have changed in two decades.

That year a graduate student at Cornell University let loose the first Internet worm, which over a period of 10 or 12 hours clogged enough machines and started putting enough traffic on the network that the network was bogged down and useless for any activity. So researchers around the country that were responsible for really putting Internet together, along with their sponsors in D.C., which at the time was the Defense Advanced Research Projects Agency (DARPA), sort of self-mobilized and understood they needed to capture this piece of malicious code. They reverse engineered it, they understood what vulnerabilities it was exploiting, and they got patches out to everybody. Following that event eventually, the network was up and running.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130295&source=rss_topic1

• **A saga of financial network security vulnerabilities**

Despite financial institutions taking sensible precautions and employing the latest technologies, the exploits of a young hacker exposes flaws in the system, Wired first reported.

Court records obtained by Wired show how Israeli-born hacker Ehud Tenenbaum and his cohorts, using SQL attacks and obtaining administrative passwords, were able to break into the networks of several financial institutions in the United States to steal confidential personal information, which they then sold via the internet. This data was copied onto counterfeit credit cards and used at ATMs to withdraw cash,

Tenenbaum, 29, also known as "The Analyzer," gained notoriety 10 years ago when he broke into computer networks of NASA, the Pentagon and the Knesset, the legislative branch of the Israeli government.

SC Magazine

Full Story :

<http://www.scmagazineus.com/A-saga-of-financial-network-security-vulnerabilities/article/129462/>

New Vulnerabilities Tested in SecureScout

• **18311 Mozilla Thunderbird - layout engine Denial of Service and Arbitrary Code execution (Remote File Checking)**

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Thunderbird 2.0.0.21.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=475136

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* BID: 33990

<http://www.securityfocus.com/bid/33990>

* SECUNIA: 34145

<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0772 (cve.mitre.org, nvd.nist.gov)

• 18312 OpenSSL ASN1 printing crash Vulnerability

The function ASN1_STRING_print_ex() when used to print a BMPString or UniversalString will crash with an invalid memory access if the encoded length of the string is illegal. (CVE-2009-0590)

Any OpenSSL application which prints out the contents of a certificate could be affected by this bug, including SSL servers, clients and S/MIME software.

Users of OpenSSL 0.9.8 should update to 0.9.8k which contains a patch to correct this issue.

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

References:

* CONFIRM: secadv_20090325

http://www.openssl.org/news/secadv_20090325.txt

CVE Reference:

CVE-2009-0590 (cve.mitre.org, nvd.nist.gov)

• 18313 OpenSSL Incorrect Error Checking During CMS verification Vulnerability

The function CMS_verify() does not correctly handle an error condition involving malformed signed attributes. This will cause an invalid set of signed attributes to appear valid and content digests will not be checked. (CVE-2009-0591)

These malformed attributes cannot be generated without access to the signer's private key so an attacker cannot forge signatures. A valid signer could however generate an invalid signature which appears valid and later repudiate the signature.

The older PKCS#7 code is not affected.

This issue only affects CMS users: CMS is only present in OpenSSL 0.9.8h and later where it is disabled by default and 0.9.9-dev.

Users of OpenSSL CMS code should update to 0.9.8k which contains a patch to correct this issue.

Thanks to Ivan Nestlerode of IBM for reporting this issue.

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

References:

* CONFIRM: secadv_20090325

http://www.openssl.org/news/secadv_20090325.txt

CVE Reference:

CVE-2009-0591 (cve.mitre.org, nvd.nist.gov)

• 18314 OpenSSL Invalid ASN1 clearing check Vulnerability

When a malformed ASN1 structure is received it's contents are freed up and zeroed and an error condition returned. On a small number of platforms where sizeof(long) < sizeof(void *) (for example WIN64) this can cause an invalid memory access later resulting in a crash when some invalid structures are read, for example RSA public keys (CVE-2009-0789).

Any OpenSSL application which uses the public key of an untrusted certificate could be crashed by a malformed structure. Including SSL servers, clients, CA and S/MIME software.

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

Thanks to Paolo Ganci for reporting this issue.

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

References:

* CONFIRM: secadv_20090325
http://www.openssl.org/news/secadv_20090325.txt

CVE Reference:

CVE-2009-0789 (cve.mitre.org, nvd.nist.gov)

• 18315 OpenSSL Incorrect checks for malformed signatures Vulnerability

Several functions inside OpenSSL incorrectly checked the result after calling the EVP_VerifyFinal function, allowing a malformed signature to be treated as a good signature rather than as an error. This issue affected the signature checks on DSA and ECDSA keys used with SSL/TLS.

One way to exploit this flaw would be for a remote attacker who is in control of a malicious server or who can use a 'man in the middle' attack to present a malformed SSL/TLS signature from a certificate chain to a vulnerable client, bypassing validation.

The vulnerability affects the OpenSSL branch 0.9.8 and was addressed in version 0.9.8.j.

This vulnerability is tracked as CVE-2008-5077.

The OpenSSL security team would like to thank the Google Security Team for reporting this issue.

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

References:

* MISC:
<http://www.ocert.org/advisories/ocert-2008-016.html>

* CONFIRM:
<http://voodoo-circle.sourceforge.net/sa/sa-20090123-01.html>

* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-038.htm>

* CONFIRM:
<http://support.nortel.com/go/main.jsp?cscat=BLTNDETAIL&id=837653>

* GENTOO: GLSA-200902-02
<http://security.gentoo.org/glsa/glsa-200902-02.xml>

* SLACKWARE: SSA:2009-014-01
<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.544796>

* SUNALERT: 250826
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-250826-1>

* UBUNTU: USN-704-1
<http://www.ubuntulinux.org/support/documentation/usn/usn-704-1>

* NETVIGILANCE-UNKNOWN: ADV-2009-0040
<http://www.frsirt.com/english/advisories/2009/0040>

* NETVIGILANCE-UNKNOWN: ADV-2009-0289
<http://www.frsirt.com/english/advisories/2009/0289>

* NETVIGILANCE-UNKNOWN: ADV-2009-0362
<http://www.frsirt.com/english/advisories/2009/0362>

* SECUNIA: 33765
<http://secunia.com/advisories/33765>

* SECUNIA: 33338
<http://secunia.com/advisories/33338>

* SECUNIA: 33673
<http://secunia.com/advisories/33673>

* SECUNIA: 33557
<http://secunia.com/advisories/33557>

* SECUNIA: 33436
<http://secunia.com/advisories/33436>

* NETVIGILANCE-UNKNOWN: ADV-2009-0558
<http://www.vupen.com/english/advisories/2009/0558>

* CONFIRM: secadv_20090107
http://www.openssl.org/news/secadv_20090107.txt

CVE Reference:

CVE-2008-5077 (cve.mitre.org, nvd.nist.gov)

• 18316 OpenSSL DTLS implementation remote code execution Vulnerability

Andy Polyakov discovered a flaw in OpenSSL's DTLS implementation which could lead to the compromise of clients and servers with DTLS enabled.

DTLS is a datagram variant of TLS specified in RFC 4347 first supported in OpenSSL version 0.9.8. Note that the vulnerabilities do not affect SSL and TLS so only clients and servers explicitly using DTLS are affected.

Taking advantage of this flaw will permit remote code execution.

All releases of 0.9.8 prior to 0.9.8f are affected.

This vulnerability is tracked as CVE-2007-4995.

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

References:

- * BUGTRAQ: 20071012 OpenSSL Security Advisory
<http://www.securityfocus.com/archive/1/archive/1/482167/100/0/threaded>
- * CONFIRM:
http://www.openssl.org/news/secadv_20071012.txt
- * CONFIRM:
http://bugs.gentoo.org/show_bug.cgi?id=195634
- * DEBIAN: DSA-1571
<http://www.debian.org/security/2008/dsa-1571>
- * FEDORA: FEDORA-2007-725
<https://www.redhat.com/archives/fedora-package-announce/2007-October/msg00218.html>
- * GENTOO: GLSA-200710-30
<http://security.gentoo.org/glsa/glsa-200710-30.xml>
- * GENTOO: GLSA-200805-07
<http://www.gentoo.org/security/en/glsa/glsa-200805-07.xml>
- * HP: HPSBUX02296
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01299773>
- * MANDRIVA: MDKSA-2007:237
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:237>
- * REDHAT: RHSA-2007:0964
<http://www.redhat.com/support/errata/RHSA-2007-0964.html>
- * SUSE: SUSE-SR:2007:021
<http://lists.opensuse.org/opensuse-security-announce/2007-10/msg00006.html>
- * UBUNTU: USN-534-1
<http://www.ubuntulinux.org/support/documentation/usn/usn-534-1>
- * BID: 26055
<http://www.securityfocus.com/bid/26055>
- * NETVIGILANCE-UNKNOWN: ADV-2007-3487
<http://www.frst.com/english/advisories/2007/3487>
- * NETVIGILANCE-UNKNOWN: ADV-2007-4219
<http://www.frst.com/english/advisories/2007/4219>
- * SECTRACK: 1018810
<http://securitytracker.com/id?1018810>
- * SECUNIA: 25878
<http://secunia.com/advisories/25878>
- * SECUNIA: 27205
<http://secunia.com/advisories/27205>
- * SECUNIA: 27217
<http://secunia.com/advisories/27217>
- * SECUNIA: 27271
<http://secunia.com/advisories/27271>
- * SECUNIA: 27363
<http://secunia.com/advisories/27363>
- * SECUNIA: 27434
<http://secunia.com/advisories/27434>
- * SECUNIA: 27933
<http://secunia.com/advisories/27933>
- * SECUNIA: 28084
<http://secunia.com/advisories/28084>
- * SECUNIA: 30161

<http://secunia.com/advisories/30161>

* SECUNIA: 30220

<http://secunia.com/advisories/30220>

* XF: openssl-dtls-code-execution(37185)

<http://xforce.iss.net/xforce/xfdb/37185>

CVE Reference:

CVE-2007-4995 (cve.mitre.org, nvd.nist.gov)

• 18317 Mozilla Thunderbird - layout engine Denial of Service and Arbitrary Code execution (CVE-2009-0771) (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Thunderbird 2.0.0.21.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

* CONFIRM:

https://bugzilla.mozilla.org/buglist.cgi?bug_id=424276,435209,436965,460706,466057,468578,471594,472502

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2009-069.htm>

* DEBIAN: DSA-1751

<http://www.debian.org/security/2009/dsa-1751>

* MANDRIVA: MDVSA-2009:075

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:075>

* SUSE: SUSE-SA:2009:012

<http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00002.html>

* BID: 33990

<http://www.securityfocus.com/bid/33990>

* SECUNIA: 34145

<http://secunia.com/advisories/34145>

* SECUNIA: 34272

<http://secunia.com/advisories/34272>

* SECUNIA: 34383

<http://secunia.com/advisories/34383>

* NETVIGILANCE-UNKNOWN: ADV-2009-0632

<http://www.vupen.com/english/advisories/2009/0632>

CVE Reference:

CVE-2009-0771 (cve.mitre.org, nvd.nist.gov)

• 18318 Mozilla Firefox - layout engine Denial of Service and Arbitrary Code execution (CVE-2009-0771) (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue impacts Firefox branch 3.x and has been fixed in version 3.0.7.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

* CONFIRM:

https://bugzilla.mozilla.org/buglist.cgi?bug_id=424276,435209,436965,460706,466057,468578,471594,472502

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2009-069.htm>

* DEBIAN: DSA-1751
<http://www.debian.org/security/2009/dsa-1751>
* MANDRIVA: MDVSA-2009:075
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:075>
* SUSE: SUSE-SA:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00002.html>
* BID: 33990
<http://www.securityfocus.com/bid/33990>
* SECUNIA: 34145
<http://secunia.com/advisories/34145>
* SECUNIA: 34272
<http://secunia.com/advisories/34272>
* SECUNIA: 34383
<http://secunia.com/advisories/34383>
* NETVIGILANCE-UNKNOWN: ADV-2009-0632
<http://www.vupen.com/english/advisories/2009/0632>

CVE Reference:

CVE-2009-0771 (cve.mitre.org, nvd.nist.gov)

• 18319 Mozilla Firefox - ignored HTTP directives (Remote File Checking)

Paul Nel reported that certain HTTP directives to not cache web pages, Cache-Control: no-store and Cache-Control: no-cache for HTTPS pages, were being ignored by Firefox 3. On a shared system, applications relying upon these HTTP directives could potentially expose private data. Another user on the system could use this vulnerability to view improperly cached pages containing private data by navigating the browser back.

The issue impacts Firefox branch 3.x and has been fixed in version 3.0.6.

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

References:

* MISC:
<http://blogs.imeta.co.uk/JDeabill/archive/2008/07/14/303.aspx>
* CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-06.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=441751
* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-040.htm>
* FEDORA: FEDORA-2009-1399
<https://www.redhat.com/archives/fedora-package-announce/2009-February/msg00240.html>
* MANDRIVA: MDVSA-2009:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:044>
* REDHAT: RHSA-2009:0256
<http://rhn.redhat.com/errata/RHSA-2009-0256.html>
* UBUNTU: USN-717-1
<http://www.ubuntu.com/usn/usn-717-1>
* BID: 33598
<http://www.securityfocus.com/bid/33598>
* SECUNIA: 33831
<http://secunia.com/advisories/33831>
* SECUNIA: 33841
<http://secunia.com/advisories/33841>
* SECUNIA: 33846
<http://secunia.com/advisories/33846>
* NETVIGILANCE-UNKNOWN: ADV-2009-0313
<http://www.frst.com/english/advisories/2009/0313>
* SECTRACK: 1021667
<http://www.securitytracker.com/id?1021667>
* SECUNIA: 33799
<http://secunia.com/advisories/33799>
* SECUNIA: 33809
<http://secunia.com/advisories/33809>
* SECUNIA: 33869
<http://secunia.com/advisories/33869>

CVE Reference:

CVE-2009-0358 (cve.mitre.org, nvd.nist.gov)

• 18320 Mozilla Firefox - XMLHttpRequest allows reading HTTPOnly cookies (Remote File Checking)

Developer and Mozilla community member Wladimir Palant reported that cookies marked HTTPOnly were readable by JavaScript via the XMLHttpRequest.getResponseHeader and XMLHttpRequest.getAllResponseHeaders APIs. This vulnerability bypasses the security mechanism provided by the HTTPOnly flag which intends to restrict JavaScript access to document.cookie.

The fix prevents the XMLHttpRequest feature from accessing the Set-Cookie and Set-Cookie2 headers of any response whether or not the HTTPOnly flag was set for those cookies.

The issue impacts Firefox branch 3.x and has been fixed in version 3.0.6.

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

References:

* MISC:

<http://ha.ckers.org/blog/20070511/bluehat-errata/>

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-05.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=380418

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2009-040.htm>

* FEDORA: FEDORA-2009-1399

<https://www.redhat.com/archives/fedora-package-announce/2009-February/msg00240.html>

* MANDRIVA: MDVSA-2009:044

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:044>

* REDHAT: RHSA-2009:0256

<http://rhn.redhat.com/errata/RHSA-2009-0256.html>

* REDHAT: RHSA-2009:0257

<http://www.redhat.com/support/errata/RHSA-2009-0257.html>

* UBUNTU: USN-717-1

<http://www.ubuntu.com/usn/usn-717-1>

* UBUNTU: USN-717-2

<http://www.ubuntu.com/usn/usn-717-2>

* BID: 33598

<http://www.securityfocus.com/bid/33598>

* SECUNIA: 33831

<http://secunia.com/advisories/33831>

* SECUNIA: 33841

<http://secunia.com/advisories/33841>

* SECUNIA: 33846

<http://secunia.com/advisories/33846>

* NETVIGILANCE-UNKNOWN: ADV-2009-0313

<http://www.frsirt.com/english/advisories/2009/0313>

* SECTRACK: 1021668

<http://www.securitytracker.com/id?1021668>

* SECUNIA: 33799

<http://secunia.com/advisories/33799>

* SECUNIA: 33808

<http://secunia.com/advisories/33808>

* SECUNIA: 33809

<http://secunia.com/advisories/33809>

* SECUNIA: 33816

<http://secunia.com/advisories/33816>

* SECUNIA: 33869

<http://secunia.com/advisories/33869>

CVE Reference:

CVE-2009-0357 (cve.mitre.org, nvd.nist.gov)

CVE-2009-0357 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- CVE-2009-1043 Microsoft CVSS 2.0 Score = 10.0

Unspecified vulnerability in Microsoft Internet Explorer 8 on Windows 7 allows remote attackers to execute arbitrary code via unknown vectors triggered by clicking on a link, as demonstrated by Nils during a PWN2OWN competition at CanSecWest 2009.

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

References:

BID: <http://www.securityfocus.com/bid/34182>

MISC: <http://www.h-online.com/security/Pwn2Own-2009-Safari-IE-8-and-Firefox-exploited--/news/112889>

MISC: http://news.cnet.com/8301-1009_3-10199652-83.html

MISC: <http://dvlabs.tippingpoint.com/blog/2009/03/20/pwn2own-day-2>

MISC:

<http://dvlabs.tippingpoint.com/blog/2009/03/18/pwn2own-2009-day-1---safari-internet-explorer-and-firefox-taken-down-by-f>

MISC: <http://dvlabs.tippingpoint.com/blog/2009/02/25/pwn2own-2009>

MISC: <http://cansecwest.com/index.html>

MISC: <http://blogs.zdnet.com/security/?p=2934>

CVE Reference: [CVE-2009-1043](https://cve.mitre.org/cve/2009/1043)

• **CVE-2008-6505 Apache CVSS 2.0 Score = 5.0**

Multiple directory traversal vulnerabilities in Apache Struts 2.0.x before 2.0.12 and 2.1.x before 2.1.3 allow remote attackers to read arbitrary files via a `../%252f` (encoded dot dot slash) in a URI with a `/struts/` path, related to (1) `FilterDispatcher` in 2.0.x and (2) `DefaultStaticContentLoader` in 2.1.x.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2008/3003>

BID: <http://www.securityfocus.com/bid/32104>

CONFIRM: <http://struts.apache.org/2.x/docs/s2-004.html>

SECUNIA: <http://secunia.com/advisories/32497>

CONFIRM: <http://issues.apache.org/struts/browse/WW-2779>

CVE Reference: [CVE-2008-6505](https://cve.mitre.org/cve/2008/6505)

• **CVE-2009-0920 HP CVSS 2.0 Score = 7.5**

Stack-based buffer overflow in `OvCgi/Toolbar.exe` in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via a long `OvOSLocale` cookie, a variant of CVE-2008-0067.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/49364>

VUPEN: <http://www.vupen.com/english/advisories/2009/0819>

SECTRACK: <http://www.securitytracker.com/id?1021883>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/502054/100/0/threaded>

MISC: <http://www.coresecurity.com/content/openview-buffer-overflows>

SECUNIA: <http://secunia.com/advisories/34444>

HP: <http://marc.info/?l=bugtraq&m=123791084113871&w=2>

HP: <http://marc.info/?l=bugtraq&m=123791084113871&w=2>

CVE Reference: [CVE-2009-0920](#)

• **CVE-2009-0921 HP CVSS 2.0 Score = 7.5**

Multiple heap-based buffer overflows in OvCgi/Toolbar.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allow remote attackers to execute arbitrary code via (1) a long OvAcceptLang cookie, which triggers the error in ov.dll and ovwww.dll, or (2) a long Accept-Language HTTP header, which triggers the error in ovwww.dll or libovwww.so.4.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/49363>

VUPEN: <http://www.vupen.com/english/advisories/2009/0819>

SECTRAK: <http://www.securitytracker.com/id?1021883>

BID: <http://www.securityfocus.com/bid/34135>

BID: <http://www.securityfocus.com/bid/34134>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/502054/100/0/threaded>

MISC: <http://www.coresecurity.com/content/openview-buffer-overflows>

SECUNIA: <http://secunia.com/advisories/34444>

HP: <http://marc.info/?l=bugtraq&m=123791084113871&w=2>

HP: <http://marc.info/?l=bugtraq&m=123791084113871&w=2>

CVE Reference: [CVE-2009-0921](#)

• **CVE-2009-0207 HP CVSS 2.0 Score = 6.8**

Unspecified vulnerability in HP-UX B.11.11 running VERITAS Oracle Disk Manager (VRTSodm) 3.5, B.11.23 running VRTSodm 4.1 or VERITAS File System (VRTSvxf) 4.1, B.11.23 running VRTSodm 5.0 or VRTSvxf 5.0, and B.11.31 running VRTSodm 5.0 allows local users to gain root privileges via unknown vectors.

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

References:

BID: <http://www.securityfocus.com/bid/34226>

HP: <http://marc.info/?l=bugtraq&m=123792744311063&w=2>

HP: <http://marc.info/?l=bugtraq&m=123792744311063&w=2>

CVE Reference: [CVE-2009-0207](#)

• **CVE-2009-0215 IBM CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in the GetXMLValue method in the IBM Access Support ActiveX control in IbmEgath.dll, as distributed on IBM and Lenovo computers, allows remote attackers to execute arbitrary code via unspecified vectors.

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

References:

CERT-VN: <http://www.kb.cert.org/vuls/id/340420>

VUPEN: <http://www.vupen.com/english/advisories/2009/0824>

BID: <http://www.securityfocus.com/bid/34228>

CVE Reference: [CVE-2009-0215](#)

• **CVE-2009-0891 IBM CVSS 2.0 Score = 5.5**

The Web Services Security component in IBM WebSphere Application Server 7.0 before Fix Pack 1 (7.0.0.1), 6.1 before Fix Pack 23 (6.1.0.23), and 6.0.2 before Fix Pack 33 (6.0.2.33) does not properly enforce (1) nonce and (2)

timestamp expiration values in WS-Security bindings as stored in the com.ibm.wsspi.wssecurity.core custom property, which allows remote authenticated users to conduct session hijacking attacks.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27014463>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27007951>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27006876>

XF: <http://xforce.iss.net/xforce/xfdb/49391>

AIXAPAR: <http://www-1.ibm.com/support/search.wss?rs=0&q=PK66676&apar=only>

CVE Reference: [CVE-2009-0891](#)

• **CVE-2009-1056 IBM CVSS 2.0 Score = 5.0**

IBM Rational AppScan Enterprise before 5.5 FP1 allows remote attackers to read arbitrary exported reports by "forcefully browsing."

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

References:

BID: <http://www.securityfocus.com/bid/34163>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PK79991>

SECUNIA: <http://secunia.com/advisories/34349>

CVE Reference: [CVE-2009-1056](#)

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