

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Apache Chunked Encoding buffer overflow.

Download Here:

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

This Week in Review

2010 worms are mostly AutoRun's. Microsoft working on fixing Windows 7 hole. A new online advertisement scam. Rogue ISP to pay back earnings.

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

• AutoRun worms most common malware during Q1 2010

Portable storage device threats, such as AutoRun worms, were the most prevalent type of malware worldwide during the first quarter of the year, according to a McAfee report issued Tuesday. Two of the top five most prevalent pieces of malware during the quarter spread via the Windows AutoRun feature, according to McAfee's Q1 Threats Report. Cybercriminals use AutoRun to automatically install malicious software on a user's PC when an infected removable storage device is plugged in. The notorious Conficker worm spread this way.

"It does not require the user to click on it, which makes it particularly dangerous," Dave Marcus, director security of research and communications at McAfee Avert Labs, told SCMagazineUS.com on Tuesday.

The threat vector is prevalent due to the widespread use of USB drives by consumers and enterprises, he said. sc Magazine

Full Story :

http://www.scmagazineus.com/autorun-worms-most-common-malware-during-q1-2010/article/170457/?utm_source=

- **Microsoft warns of 64-bit Windows 7 hole**

(Credit: Microsoft)

Microsoft is working on a patch to fix a hole in a 64-bit Windows 7 graphics display component that could be exploited to crash the system or potentially take control of the computer by running code remotely.

The company is investigating a new publicly reported vulnerability in the Windows Canonical Display Driver (cdd.dll) that affects 64-bit versions of Windows 7 and Windows Server 2008 R2, and Itanium-based Windows Server 2008 R2. The driver enables applications to use graphics and formatted text on the video display and printer. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20005420-245.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Microsoft files two lawsuits for "click laundering"**

Microsoft this week filed two lawsuits in federal court in Seattle against alleged perpetrators of a new, technologically advanced form of online advertising click fraud being dubbed "click laundering."

According to Microsoft, click fraud is an online advertising scam that occurs when a person or computer program imitates a legitimate user and clicks on an online ad for the purpose of generating a fraudulent "charge-per-click," without having any interest in the ad.

Click laundering, meanwhile, is a more advanced form of click fraud designed to outwit fraud detection systems by hiding the origin of fake clicks. SC Magazine

Full Story :

http://www.scmagazineus.com/microsoft-files-two-lawsuits-for-click-laundering/article/170621/?utm_source=feedburn

- **Rogue web host assets to be sold, must pay FTC \$1.1M**

A U.S. District Court judge has ordered the shuttering of a rogue internet service provider (ISP) accused of participating in the distribution of spam, spyware and child pornography, the Federal Trade Commission (FTC) announced Thursday.

Assets belonging to the California-based ISP, named Pricewert LLC but which does business as 3FN, have been seized and will be sold. In addition, the former business must pay the FTC \$1.08 million in ill-gotten gains.

The permanent shutdown order comes following a temporary restraining order issued last June that froze 3FN's assets and directed its upstream internet providers and data centers to stop providing services to 3FN. SC Magazine

Full Story :

http://www.scmagazineus.com/rogue-web-host-assets-to-be-sold-must-pay-ftc-11m/article/170622/?utm_source=feedburn

New Vulnerabilities Tested in SecureScout

- **18803 Mozilla Firefox - Deleted frame reuse in multipart/x-mixed-replace image (Remote File Checking)**

Security researcher regenrecht reported (via TippingPoint's Zero Day Initiative) a potential reuse of a deleted image frame in Firefox 3.6's handling of multipart/x-mixed-replace images. Although no exploit was shown, re-use of freed memory has led to exploitable vulnerabilities in the past.

The issue has been fixed in Firefox 3.6.2.

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

References:

* BUGTRAQ: 20100402 ZDI-10-047: Mozilla Firefox libprOn imgContainer Bits-Per-Pixel Change Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/510535/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-047>

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-09.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=547143

* MANDRIVA: MDVSA-2010:070

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>

* BID: 38918
<http://www.securityfocus.com/bid/38918>
* BID: 38921
<http://www.securityfocus.com/bid/38921>
* VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0164 (cve.mitre.org, nvd.nist.gov)

• 18804 Mozilla Firefox - WOFF heap corruption due to integer overflow (Remote File Checking)

Security researcher Evgeny Legerov of Intevydis reported that the WOFF decoder contains an integer overflow in a font decompression routine. This flaw could result in too small a memory buffer being allocated to store a downloadable font. An attacker could use this vulnerability to crash a victim's browser and execute arbitrary code on his/her system.

The issue has been fixed in Firefox 3.6.2.

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

References:

* MISC:
<http://blog.mozilla.com/security/2010/02/22/secunia-advisory-sa38608/>
* MISC:
<http://blog.psi2.de/en/2010/02/20/going-commercial-with-firefox-vulnerabilities/>
* MISC:
<http://secunia.com/community/forum/thread/show/3592>
* MISC:
<http://www.h-online.com/security/news/item/Zero-day-exploit-for-Firefox-3-6-936124.html>
* MISC:
<https://forum.immunityinc.com/board/thread/1161/vulndisco-9-0/>
* CONFIRM:
<http://blog.mozilla.com/security/2010/03/18/update-on-secunia-advisory-sa38608/>
* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-08.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=552216
* CERT-VN: VU#964549
<http://www.kb.cert.org/vuls/id/964549>
* SECUNIA: 38608
<http://secunia.com/advisories/38608>

CVE Reference:

CVE-2010-1028 (cve.mitre.org, nvd.nist.gov)

• 18805 Mozilla Thunderbird - SSPI authentication crash (Remote File Checking)

The nsAuthSSPI::Unwrap function in extensions/auth/nsAuthSSPI.cpp in Mozilla Thunderbird before 2.0.0.24 on Windows Vista, Windows Server 2008 R2, and Windows 7 allows remote SMTP, IMAP, and POP servers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via crafted data in a session that uses SSPI.

The issue has been fixed in Thunderbird 2.0.0.24.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-07.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=511806
* BID: 38831
<http://www.securityfocus.com/bid/38831>
* SECUNIA: 39001
<http://secunia.com/advisories/39001>
* VUPEN: ADV-2010-0648
<http://www.vupen.com/english/advisories/2010/0648>
* XF: thunderbird-activedirectory-dos(56992)

<http://xforce.iss.net/xforce/xfdb/56992>

CVE Reference:

CVE-2010-0161 (cve.mitre.org, nvd.nist.gov)

• 18806 Mozilla Thunderbird - Mime attachment crash (Remote File Checking)

Mozilla Thunderbird before 2.0.0.24 process e-mail attachments with a parser that performs casts and line termination incorrectly, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted message, related to message indexing.

The issue has been fixed in Thunderbird 2.0.0.24.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-07.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=505221
- * UBUNTU: USN-915-1
<http://www.ubuntu.com/usn/USN-915-1>
- * BID: 38831
<http://www.securityfocus.com/bid/38831>
- * SECUNIA: 39001
<http://secunia.com/advisories/39001>
- * SECUNIA: 38977
<http://secunia.com/advisories/38977>
- * VUPEN: ADV-2010-0648
<http://www.vupen.com/english/advisories/2010/0648>
- * XF: thunderbird-messages-dos(56993)
<http://xforce.iss.net/xforce/xfdb/56993>

CVE Reference:

CVE-2010-0163 (cve.mitre.org, nvd.nist.gov)

• 18807 Mozilla Thunderbird - JavaScript engine crash (Remote File Checking)

Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Thunderbird before 2.0.0.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to use of mutable strings in the js_StringReplaceHelper function in js/src/jsstr.cpp, and unknown vectors.

The issue has been fixed in Thunderbird 2.0.0.24.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-47.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=441714
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=505305
- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-07.html>
- * REDHAT: RHSA-2009:1430
<http://www.redhat.com/support/errata/RHSA-2009-1430.html>
- * REDHAT: RHSA-2009:1431
<http://www.redhat.com/support/errata/RHSA-2009-1431.html>
- * REDHAT: RHSA-2009:1432
<http://www.redhat.com/support/errata/RHSA-2009-1432.html>
- * REDHAT: RHSA-2010:0153
<http://www.redhat.com/support/errata/RHSA-2010-0153.html>
- * REDHAT: RHSA-2010:0154
<http://www.redhat.com/support/errata/RHSA-2010-0154.html>
- * UBUNTU: USN-915-1
<http://www.ubuntu.com/usn/USN-915-1>
- * SECUNIA: 36671

<http://secunia.com/advisories/36671>

* SECUNIA: 39001

<http://secunia.com/advisories/39001>

* SECUNIA: 38977

<http://secunia.com/advisories/38977>

* VUPEN: ADV-2010-0648

<http://www.vupen.com/english/advisories/2010/0648>

* VUPEN: ADV-2010-0650

<http://www.vupen.com/english/advisories/2010/0650>

CVE Reference:

CVE-2009-3075 (cve.mitre.org, nvd.nist.gov)

• 18808 Mozilla Thunderbird - BinHex decoder crash (Remote File Checking)

Multiple unspecified vulnerabilities in the browser engine in Thunderbird before 2.0.0.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the BinHex decoder in network/streamconv/converters/nsBinHexDecoder.cpp, and unknown vectors.

The issue has been fixed in Thunderbird 2.0.0.24.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-47.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=494283

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=501900

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=508074

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-07.html>

* REDHAT: RHSA-2009:1430

<http://www.redhat.com/support/errata/RHSA-2009-1430.html>

* REDHAT: RHSA-2009:1431

<http://www.redhat.com/support/errata/RHSA-2009-1431.html>

* REDHAT: RHSA-2009:1432

<http://www.redhat.com/support/errata/RHSA-2009-1432.html>

* REDHAT: RHSA-2010:0153

<http://www.redhat.com/support/errata/RHSA-2010-0153.html>

* REDHAT: RHSA-2010:0154

<http://www.redhat.com/support/errata/RHSA-2010-0154.html>

* UBUNTU: USN-915-1

<http://www.ubuntu.com/usn/USN-915-1>

* SECUNIA: 36671

<http://secunia.com/advisories/36671>

* SECUNIA: 39001

<http://secunia.com/advisories/39001>

* SECUNIA: 38977

<http://secunia.com/advisories/38977>

* VUPEN: ADV-2010-0648

<http://www.vupen.com/english/advisories/2010/0648>

* VUPEN: ADV-2010-0650

<http://www.vupen.com/english/advisories/2010/0650>

CVE Reference:

CVE-2009-3072 (cve.mitre.org, nvd.nist.gov)

• 18809 Mozilla Thunderbird - base64 decoding integer overflow (Remote File Checking)

Multiple integer overflows in the (1) PL_Base64Decode and (2) PL_Base64Encode functions in nsprpub/lib/libc/src/base64.c in Thunderbird before 2.0.0.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors that trigger buffer overflows.

The issue has been fixed in Thunderbird 2.0.0.24.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-34.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=492779
- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-07.html>
- * FEDORA: FEDORA-2009-7961
<https://www.redhat.com/archives/fedora-package-announce/2009-July/msg01032.html>
- * REDHAT: RHSA-2009:1162
<http://rhn.redhat.com/errata/RHSA-2009-1162.html>
- * REDHAT: RHSA-2009:1163
<http://rhn.redhat.com/errata/RHSA-2009-1163.html>
- * REDHAT: RHSA-2010:0153
<http://www.redhat.com/support/errata/RHSA-2010-0153.html>
- * REDHAT: RHSA-2010:0154
<http://www.redhat.com/support/errata/RHSA-2010-0154.html>
- * SUNALERT: 265068
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-265068-1>
- * SUSE: SUSE-SA:2009:042
<http://lists.opensuse.org/opensuse-security-announce/2009-08/msg00002.html>
- * SUSE: SUSE-SA:2009:039
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00005.html>
- * UBUNTU: USN-915-1
<http://www.ubuntu.com/usn/USN-915-1>
- * BID: 35758
<http://www.securityfocus.com/bid/35758>
- * SECUNIA: 35914
<http://secunia.com/advisories/35914>
- * SECUNIA: 35943
<http://secunia.com/advisories/35943>
- * SECUNIA: 35944
<http://secunia.com/advisories/35944>
- * SECUNIA: 35947
<http://secunia.com/advisories/35947>
- * SECUNIA: 36145
<http://secunia.com/advisories/36145>
- * SECUNIA: 36005
<http://secunia.com/advisories/36005>
- * SECUNIA: 39001
<http://secunia.com/advisories/39001>
- * SECUNIA: 38977
<http://secunia.com/advisories/38977>
- * VUPEN: ADV-2009-1972
<http://www.vupen.com/english/advisories/2009/1972>
- * VUPEN: ADV-2009-2152
<http://www.vupen.com/english/advisories/2009/2152>
- * VUPEN: ADV-2010-0648
<http://www.vupen.com/english/advisories/2010/0648>
- * VUPEN: ADV-2010-0650
<http://www.vupen.com/english/advisories/2010/0650>

CVE Reference:

CVE-2009-2463 (cve.mitre.org, nvd.nist.gov)

• 18810 Mozilla Firefox - JavaScript engine crash (Remote File Checking)

Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox before 3.0.14 and 3.5.x before 3.5.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to use of mutable strings in the `js_StringReplaceHelper` function in `js/src/jsstr.cpp`, and unknown vectors.

The issue has been fixed in Firefox 3.0.14 and 3.5.2.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-47.html>

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=441714
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=505305
* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-07.html>
* REDHAT: RHSA-2009:1430
<http://www.redhat.com/support/errata/RHSA-2009-1430.html>
* REDHAT: RHSA-2009:1431
<http://www.redhat.com/support/errata/RHSA-2009-1431.html>
* REDHAT: RHSA-2009:1432
<http://www.redhat.com/support/errata/RHSA-2009-1432.html>
* REDHAT: RHSA-2010:0153
<http://www.redhat.com/support/errata/RHSA-2010-0153.html>
* REDHAT: RHSA-2010:0154
<http://www.redhat.com/support/errata/RHSA-2010-0154.html>
* UBUNTU: USN-915-1
<http://www.ubuntu.com/usn/USN-915-1>
* SECUNIA: 36671
<http://secunia.com/advisories/36671>
* SECUNIA: 39001
<http://secunia.com/advisories/39001>
* SECUNIA: 38977
<http://secunia.com/advisories/38977>
* VUPEN: ADV-2010-0648
<http://www.vupen.com/english/advisories/2010/0648>
* VUPEN: ADV-2010-0650
<http://www.vupen.com/english/advisories/2010/0650>

CVE Reference:

CVE-2009-3075 (cve.mitre.org, nvd.nist.gov)

• 18811 Mozilla Firefox - BinHex decoder crash (Remote File Checking)

Multiple unspecified vulnerabilities in the browser engine in Firefox before 3.0.14 and 3.5.x before 3.5.3 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the BinHex decoder in network/streamconv/converters/nsBinHexDecoder.cpp, and unknown vectors.

The issue has been fixed in Firefox 3.0.14 and 3.5.3.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-47.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=494283
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=501900
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=508074
* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-07.html>
* REDHAT: RHSA-2009:1430
<http://www.redhat.com/support/errata/RHSA-2009-1430.html>
* REDHAT: RHSA-2009:1431
<http://www.redhat.com/support/errata/RHSA-2009-1431.html>
* REDHAT: RHSA-2009:1432
<http://www.redhat.com/support/errata/RHSA-2009-1432.html>
* REDHAT: RHSA-2010:0153
<http://www.redhat.com/support/errata/RHSA-2010-0153.html>
* REDHAT: RHSA-2010:0154
<http://www.redhat.com/support/errata/RHSA-2010-0154.html>
* UBUNTU: USN-915-1
<http://www.ubuntu.com/usn/USN-915-1>
* SECUNIA: 36671
<http://secunia.com/advisories/36671>
* SECUNIA: 39001

<http://secunia.com/advisories/39001>

* SECUNIA: 38977

<http://secunia.com/advisories/38977>

* VUPEN: ADV-2010-0648

<http://www.vupen.com/english/advisories/2010/0648>

* VUPEN: ADV-2010-0650

<http://www.vupen.com/english/advisories/2010/0650>

CVE Reference:

CVE-2009-3072 (cve.mitre.org, nvd.nist.gov)

• 18812 Mozilla Firefox - base64 decoding integer overflow (Remote File Checking)

Multiple integer overflows in the (1) PL_Base64Decode and (2) PL_Base64Encode functions in nsprpub/lib/libc/src/base64.c in Firefox before 3.0.12 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors that trigger buffer overflows.

The issue has been fixed in Firefox 3.0.12.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-34.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=492779

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-07.html>

* FEDORA: FEDORA-2009-7961

<https://www.redhat.com/archives/fedora-package-announce/2009-July/msg01032.html>

* REDHAT: RHSA-2009:1162

<http://rhn.redhat.com/errata/RHSA-2009-1162.html>

* REDHAT: RHSA-2009:1163

<http://rhn.redhat.com/errata/RHSA-2009-1163.html>

* REDHAT: RHSA-2010:0153

<http://www.redhat.com/support/errata/RHSA-2010-0153.html>

* REDHAT: RHSA-2010:0154

<http://www.redhat.com/support/errata/RHSA-2010-0154.html>

* SUNALERT: 265068

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-265068-1>

* SUSE: SUSE-SA:2009:042

<http://lists.opensuse.org/opensuse-security-announce/2009-08/msg00002.html>

* SUSE: SUSE-SA:2009:039

<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00005.html>

* UBUNTU: USN-915-1

<http://www.ubuntu.com/usn/USN-915-1>

* BID: 35758

<http://www.securityfocus.com/bid/35758>

* SECUNIA: 35914

<http://secunia.com/advisories/35914>

* SECUNIA: 35943

<http://secunia.com/advisories/35943>

* SECUNIA: 35944

<http://secunia.com/advisories/35944>

* SECUNIA: 35947

<http://secunia.com/advisories/35947>

* SECUNIA: 36145

<http://secunia.com/advisories/36145>

* SECUNIA: 36005

<http://secunia.com/advisories/36005>

* SECUNIA: 39001

<http://secunia.com/advisories/39001>

* SECUNIA: 38977

<http://secunia.com/advisories/38977>

* VUPEN: ADV-2009-1972

<http://www.vupen.com/english/advisories/2009/1972>

* VUPEN: ADV-2009-2152

<http://www.vupen.com/english/advisories/2009/2152>

* VUPEN: ADV-2010-0648
<http://www.vupen.com/english/advisories/2010/0648>
* VUPEN: ADV-2010-0650
<http://www.vupen.com/english/advisories/2010/0650>

CVE Reference:

CVE-2009-2463 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-0775 IBM CVSS 2.0 Score = 5.0

Unspecified vulnerability in IBM WebSphere Application Server (WAS) 6.0 before 6.0.2.41, 6.1 before 6.1.0.31, and 7.0 before 7.0.0.11 allows remote attackers to cause a denial of service (memory consumption and daemon crash) via a crafted request, related to the nodeagent and Deployment Manager components.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/58555>

CVE Reference: [CVE-2010-0775](#)

• CVE-2010-0776 IBM CVSS 2.0 Score = 5.0

The Web Container in IBM WebSphere Application Server (WAS) 6.0 before 6.0.2.43, 6.1 before 6.1.0.31, and 7.0 before 7.0.0.11 does not properly handle chunked transfer encoding during a call to response.sendRedirect, which allows remote attackers to cause a denial of service via a GET request.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/58556>

CVE Reference: [CVE-2010-0776](#)

• CVE-2010-0774 IBM CVSS 2.0 Score = 4.3

The (1) JAX-RPC WS-Security 1.0 and (2) JAX-WS runtime implementations in IBM WebSphere Application Server (WAS) 6.0 before 6.0.2.41, 6.1 before 6.1.0.31, and 7.0 before 7.0.0.11 do not properly handle WebServices PKCS#7 and PKIPath tokens, which allows remote attackers to bypass intended access restrictions via unspecified vectors.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/58554>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PK96427>

CVE Reference: [CVE-2010-0774](#)

• CVE-2010-0777 IBM CVSS 2.0 Score = 2.6

The Web Container in IBM WebSphere Application Server (WAS) 6.0 before 6.0.2.43, 6.1 before 6.1.0.31, and 7.0 before 7.0.0.11 does not properly handle long filenames and consequently sends an incorrect file in some responses, which allows remote attackers to obtain sensitive information by reading the retrieved file.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/58557>

CVE Reference: [CVE-2010-0777](#)

• CVE-2010-1169 PostgreSQL CVSS 2.0 Score = 8.5

PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 does not properly restrict PL/perl procedures, which allows remote authenticated users, with database-creation privileges, to execute arbitrary Perl code via a crafted script, related to the Safe module (aka Safe.pm) for Perl.

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

References:

CONFIRM: <http://www.postgresql.org/about/news.1203>
CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=582615
VUPEN: <http://www.vupen.com/english/advisories/2010/1167>
BID: <http://www.securityfocus.com/bid/40215>
CONFIRM: <http://www.postgresql.org/support/security>
CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-4-4.html>
CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-3-11.html>
CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-2-17.html>
CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-1-21.html>
CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-0-25.html>
CONFIRM: <http://www.postgresql.org/docs/current/static/release-7-4-29.html>
SECUNIA: <http://secunia.com/advisories/39845>

CVE Reference: [CVE-2010-1169](#)

• **CVE-2010-1447 PostgreSQL CVSS 2.0 Score = 8.5**

PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 does not properly restrict PL/perl procedures, which might allow remote attackers to execute arbitrary Perl code via a crafted script, related to the Safe module (aka Safe.pm) for Perl.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/1167>
CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=588269
CONFIRM: <https://bugs.launchpad.net/bugs/cve/2010-1447>
CONFIRM: <http://www.postgresql.org/about/news.1203>
CONFIRM: <http://security-tracker.debian.org/tracker/CVE-2010-1447>
SECUNIA: <http://secunia.com/advisories/39845>

CVE Reference: [CVE-2010-1447](#)

• **CVE-2010-1170 PostgreSQL CVSS 2.0 Score = 6.0**

The PL/Tcl implementation in PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 loads Tcl code from the pltcl_modules table regardless of the table's ownership and permissions, which allows remote authenticated users, with database-creation privileges, to execute arbitrary Tcl code by creating this table and inserting a crafted Tcl script.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/1167>
CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=583072
BID: <http://www.securityfocus.com/bid/40215>
CONFIRM: <http://www.postgresql.org/support/security>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-4-4.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-3-11.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-2-17.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-1-21.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-0-25.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-7-4-29.html>

CONFIRM: <http://www.postgresql.org/about/news.1203>

SECUNIA: <http://secunia.com/advisories/39845>

CVE Reference: [CVE-2010-1170](#)

• **CVE-2010-1975 PostgreSQL CVSS 2.0 Score = 5.5**

PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, and 8.4 before 8.4.4 does not properly check privileges during certain RESET ALL operations, which allows remote authenticated users to remove arbitrary parameter settings via a (1) ALTER USER or (2) ALTER DATABASE statement.

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

References:

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-4-4.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-3-11.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-2-17.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-1-21.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-8-0-25.html>

CONFIRM: <http://www.postgresql.org/docs/current/static/release-7-4-29.html>

CVE Reference: [CVE-2010-1975](#)

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