

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

Beware of phone based attacks. Android lacks security. Verisign and Comodo fighting. Twitter to better security.

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

• SMBs, individuals being targeted by telephone DoS

If your phone starts ringing off the hook, there is a chance cybercriminals are draining your bank or online trading account at the exact same moment, the FOB warned Monday.

Online vandals increasingly are leveraging telephone-based denial-of-service (DoS) attacks to tie up the phone lines of unsuspecting individuals as they simultaneously plunder bank accounts, the FBI said in an advisory. The perpetrators use automated-dialing programs to deliver constant phone call phone calls to a target's number.

"Turns out the calls are simply a diversionary tactic: While the lines are tied up, the criminals - masquerading as the victims themselves - are raiding the victims' bank accounts or other money management accounts," the FBI said. sc Magazine

Full Story :

http://www.scmagazineus.com/smb-s-individuals-being-targeted-by-telephone-dos/article/172962/?utm_source=feedl

• Report: A fifth of Android apps expose private data

(Credit: Android) About 20 percent of the 48,000 apps in the Android marketplace allow a third-party application access to sensitive or private information, according to a report released on Tuesday.

And some of the apps were found to have the ability to do things like make calls and send text messages without the mobile user doing anything. For instance, 5 percent of the apps can place calls to any number and 2 percent can allow an app to send unknown SMS messages to premium numbers that incur expensive charges, security firm SMOBILE Systems concluded in its Android market threat report.

Meanwhile, dozens of apps were found to have the same type of access to sensitive information as known spyware does, including access to the content of e-mails and text messages, phone call information, and device location, said Dan Hoffman, chief technology officer at SMOBILE Systems. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20008518-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• VeriSign refutes competitor's vulnerability claim

VeriSign and rival Comodo are at odds over whether the process by which users can access VeriSign SSL customer account constitutes a vulnerability. Through a Google search query, Comodo employees last week discovered the certificate request page for Bank of America, a VeriSign customer, Melih Abdulhayoglu, CEO and president of Comodo, told SCMagazineUS.com on Wednesday.

"Why are you making your security application accessible by Google?" Abdulhayoglu said. "That's security architecture 101. You don't let Google index important information like that. It serves no purpose whatsoever."

A Bank of America spokesperson could not immediately be reached for comment. SC Magazine

Full Story :

http://www.scmagazineus.com/verisign-refutes-competitors-vulnerability-claim/article/173095/?utm_source=feedburner

• FTC forces Twitter to upgrade its IT security program

In an agency first, the Federal Trade Commission (FTC) has settled with a social networking provider over charges that the popular website failed to properly safeguard the data and privacy of its users.

The settlement with Twitter resolves a complaint that the microblogging service committed a number of snafus that led to users' accounts being compromised to deliver bogus tweets to followers. In one case, attackers were able to exert administrative control over the site, which enabled them to deliver bogus tweets pretending to originate from the accounts of a number of well-known members, including President Obama.

In its complaint, the FTC contended that between January and May 2009, hackers "were able to view nonpublic user information, gain access to direct messages and protected tweets, and reset any user's password and send authorized tweets from any user account," according to a news release issued Thursday. SC Magazine

Full Story :

http://www.scmagazineus.com/ftc-forces-twitter-to-upgrade-its-it-security-program/article/173169/?utm_source=feedburner

New Vulnerabilities Tested in SecureScout

• 18838 Excel Record Stack Corruption Vulnerability (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* VUPEN: VUPEN/ADV-2010-1395

<http://www.vupen.com/english/advisories/2010/1395>

* SECTRACK: 1024076

<http://securitytracker.com/alerts/2010/Jun/1024076.html>

* MS: MS10-038

<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

* BID: 40529

<http://www.securityfocus.com/bid/40529>

CVE Reference:

CVE-2010-1251 (cve.mitre.org, nvd.nist.gov)

• 18839 Excel String Variable Vulnerability (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * VUPEN: VUPEN/ADV-2010-1395
<http://www.vupen.com/english/advisories/2010/1395>
- * SECTRAK: 1024076
<http://securitytracker.com/alerts/2010/Jun/1024076.html>
- * MS: MS10-038
<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * BID: 40530
<http://www.securityfocus.com/bid/40530>

CVE Reference:

CVE-2010-1252 (cve.mitre.org, nvd.nist.gov)

• 18840 Excel ADO Object Vulnerability (MS10-038/2027452) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * VUPEN: VUPEN/ADV-2010-1395
<http://www.vupen.com/english/advisories/2010/1395>
- * SECTRAK: 1024076
<http://securitytracker.com/alerts/2010/Jun/1024076.html>
- * BUGTRAQ: 20100608 ZDI-10-103: Microsoft Office Excel DBQueryExt Record Unspecified ADO Object Remote Code Execution Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/511728/100/0/threaded>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-10-103>
- * MS: MS10-038
<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * OSVDB: 65228
<http://osvdb.org/65228>
- * BID: 40531
<http://www.securityfocus.com/bid/40531>

CVE Reference:

CVE-2010-1253 (cve.mitre.org, nvd.nist.gov)

• 18842 Help.aspx XSS Vulnerability (MS10-039/2028554) (Remote File Checking)

A cross-site scripting and spoofing vulnerability exists in Microsoft Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007 that could allow an attacker to convince a user to run a malicious script. An attacker who successfully exploited the vulnerability could modify Web browser caches and intermediate proxy server caches. Additionally, an attacker could put spoofed content into those caches. An attacker may also be able to exploit the vulnerability to perform cross-site scripting attacks.

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

References:

- * BUGTRAQ: 20100428 XSS in Microsoft SharePoint Server 2007
<http://www.securityfocus.com/archive/1/archive/1/511021/100/0/threaded>

* MISC:

http://www.htbridge.ch/advisory/xss_in_microsoft_sharepoint_server_2007.html

* MS: MS10-039

<http://www.microsoft.com/technet/security/bulletin/ms10-039.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

* SECTRAK: 1023932

<http://securitytracker.com/alerts/2010/Apr/1023932.html>

* VUPEN: VUPEN/ADV-2010-1041

<http://www.vupen.com/english/advisories/2010/1041>

* BID: 39776

<http://www.securityfocus.com/bid/39776>

CVE Reference:

CVE-2010-0817 (cve.mitre.org, nvd.nist.gov)

• 18843 toStaticHTML Information Disclosure Vulnerability (MS10-039/2028554) (Remote File Checking)

An information disclosure vulnerability exists in the way that the SharePoint toStaticHTML API sanitizes HTML, that could allow an attacker to perform cross-site scripting attacks and run script in the security context of the logged-on user.

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

References:

* SECTRAK: 1024078

<http://securitytracker.com/alerts/2010/Jun/1024078.html>

* VUPEN: VUPEN/ADV-2010-1396

<http://www.vupen.com/english/advisories/2010/1396>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100089747>

* MS: MS10-035

<http://www.microsoft.com/technet/security/bulletin/ms10-035.msp>

* MS: MS10-039

<http://www.microsoft.com/technet/security/bulletin/ms10-039.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

* BID: 40409

<http://www.securityfocus.com/bid/40409>

* XF: ie-tostatichtml-information-disclosure(58866)

<http://xforce.iss.net/xforce/xfdb/58866>

CVE Reference:

CVE-2010-1257 (cve.mitre.org, nvd.nist.gov)

• 18844 Sharepoint Help Page Denial of Service Vulnerability (MS10-039/2028554) (Remote File Checking)

A denial of service vulnerability exists in the way that Microsoft SharePoint handles specially crafted requests to the help page. An attacker could exploit the vulnerability by sending specially crafted packets to the targeted SharePoint server which could cause the Web server to become non-responsive until the associated application pool is restarted.

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

References:

* SECTRAK: 1024077

<http://securitytracker.com/alerts/2010/Jun/1024077.html>

* VUPEN: VUPEN/ADV-2010-1396

<http://www.vupen.com/english/advisories/2010/1396>

* MS: MS10-039

<http://www.microsoft.com/technet/security/bulletin/ms10-039.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

* BID: 40559

<http://www.securityfocus.com/bid/40559>

CVE Reference:

CVE-2010-1264 (cve.mitre.org, nvd.nist.gov)

• 18845 Media Decompression Vulnerability (MS10-033/979902) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Windows handles media files. This vulnerability could allow remote code execution if a user opened a specially crafted media file. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

- * SECTRAK: 1024069
<http://securitytracker.com/alerts/2010/Jun/1024069.html>
- * VUPEN: VUPEN/ADV-2010-1390
<http://www.vupen.com/english/advisories/2010/1390>
- * MS: MS10-033
<http://www.microsoft.com/technet/security/bulletin/ms10-033.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * BID: 40432
<http://www.securityfocus.com/bid/40432>

CVE Reference:

CVE-2010-1879 (cve.mitre.org, nvd.nist.gov)

• 18846 MJPEG Media Decompression Vulnerability (MS10-033/979902) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Windows handles media files. This vulnerability could allow remote code execution if a user opened a specially crafted file. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

- * SECTRAK: 1024069
<http://securitytracker.com/alerts/2010/Jun/1024069.html>
- * VUPEN: VUPEN/ADV-2010-1390
<http://www.vupen.com/english/advisories/2010/1390>
- * BID: 40432
<http://www.securityfocus.com/bid/40432>
- * MS: MS10-033
<http://www.microsoft.com/technet/security/bulletin/ms10-033.msp>
- * CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- * OSVDB: 65222
<http://osvdb.org/65222>

CVE Reference:

CVE-2010-1880 (cve.mitre.org, nvd.nist.gov)

• 18847 IIS Authentication Memory Corruption Vulnerability (MS10-040/982666) (Remote File Checking)

A remote code execution vulnerability exists in Internet Information Services (IIS). The vulnerability is due to improper parsing of authentication information. An attacker who successfully exploited this vulnerability could execute code in the context of the Worker Process Identity (WPI).

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

References:

- * SECTRAK: 1024079
<http://securitytracker.com/alerts/2010/Jun/1024079.html>
- * VUPEN: VUPEN/ADV-2010-1397
<http://www.vupen.com/english/advisories/2010/1397>
- * BID: 40432

<http://www.securityfocus.com/bid/40432>

* MS: MS10-040

<http://www.microsoft.com/technet/security/bulletin/ms10-040.msp>

* CERT: TA10-159B

<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>

* BID: 40573

<http://www.securityfocus.com/bid/40573>

* XF: ms-iis-authentication-code-execution(58864)

<http://xforce.iss.net/xforce/xfdb/58864>

CVE Reference:

CVE-2010-1256 (cve.mitre.org, nvd.nist.gov)

• 18848 XML Signature HMAC Truncation Authentication Bypass Vulnerability (MS10-041/981343) (Remote File Checking)

A data tampering vulnerability exists in the Microsoft .NET Framework that could allow an attacker to tamper with signed XML content without being detected. In custom applications, the security impact depends on the specific usage scenario. Scenarios in which signed XML messages are transmitted over a secure channel (such as SSL) are not affected by this vulnerability.

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

References:

* SECTrack: 1024080

<http://securitytracker.com/alerts/2010/Jun/1024080.html>

* VUPEN: VUPEN/ADV-2010-1398

<http://www.vupen.com/english/advisories/2010/1398>

* MISC:

http://www.w3.org/QA/2009/07/hmac_truncation_in_xml_signatu.html

* CONFIRM:

<http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg21384925>

* CONFIRM:

<http://www.aleksey.com/xmlsec/>

* CONFIRM:

<http://www.mono-project.com/Vulnerabilities>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>

* CONFIRM:

<http://www.w3.org/2008/06/xmlsigcore-errata.html#e03>

* CONFIRM:

https://issues.apache.org/bugzilla/show_bug.cgi?id=47527

* CONFIRM:

<http://www.kb.cert.org/vuls/id/MAPG-7TSKXQ>

* CONFIRM:

<http://sunsolve.sun.com/search/document.do?assetkey=1-21-125136-16-1>

* CONFIRM:

http://blogs.sun.com/security/entry/cert_vulnerability_note_vu_466161

* CONFIRM:

<http://www.kb.cert.org/vuls/id/WDON-7TY529>

* CONFIRM:

https://issues.apache.org/bugzilla/show_bug.cgi?id=47526

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html>

* CONFIRM:

<http://git.gnome.org/cgiit/xmlsec/commit/?id=34b349675af9f72eb822837a8772cc1ead7115c7>

* CONFIRM:

<http://git.gnome.org/cgiit/xmlsec/patch/?id=34b349675af9f72eb822837a8772cc1ead7115c7>

* CONFIRM:

<http://svn.apache.org/viewvc?revision=794013&view=revision>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=511915

* CONFIRM:

<http://www.openoffice.org/security/cves/CVE-2009-0217.html>

* AIXAPAR: PK80596

<http://www-01.ibm.com/support/docview.wss?rs=180&context=SSEQTP&dc=D400&uid=swg24023545&am>

* AIXAPAR: PK80627

<http://www-01.ibm.com/support/docview.wss?rs=180&context=SSEQTP&dc=D400&uid=swg24023723&am>

* APPLE: APPLE-SA-2009-09-03-1

<http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html>
* DEBIAN: DSA-1995
<http://www.debian.org/security/2010/dsa-1995>
* FEDORA: FEDORA-2009-8329
<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html>
* FEDORA: FEDORA-2009-8337
<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html>
* FEDORA: FEDORA-2009-8456
<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00494.html>
* FEDORA: FEDORA-2009-8473
<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00505.html>
* HP: HPSBUX02476
<http://marc.info/?l=bugtraq&m=125787273209737&w=2>
* MANDRIVA: MDVSA-2009:209
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:209>
* MS: MS10-041
<http://www.microsoft.com/technet/security/bulletin/ms10-041.msp>
* REDHAT: RHSA-2009:1200
<https://rhn.redhat.com/errata/RHSA-2009-1200.html>
* REDHAT: RHSA-2009:1201
<https://rhn.redhat.com/errata/RHSA-2009-1201.html>
* REDHAT: RHSA-2009:1428
<https://rhn.redhat.com/errata/RHSA-2009-1428.html>
* REDHAT: RHSA-2009:1636
<https://rhn.redhat.com/errata/RHSA-2009-1636.html>
* REDHAT: RHSA-2009:1637
<https://rhn.redhat.com/errata/RHSA-2009-1637.html>
* REDHAT: RHSA-2009:1649
<https://rhn.redhat.com/errata/RHSA-2009-1649.html>
* REDHAT: RHSA-2009:1650
<https://rhn.redhat.com/errata/RHSA-2009-1650.html>
* REDHAT: RHSA-2009:1694
<http://www.redhat.com/support/errata/RHSA-2009-1694.html>
* SUNALERT: 263429
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-263429-1>
* SUNALERT: 269208
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-269208-1>
* SUNALERT: 1020710
<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1020710.1-1>
* SUSE: SUSE-SA:2009:053
<http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00002.html>
* SUSE: SUSE-SA:2010:017
<http://lists.opensuse.org/opensuse-security-announce/2010-03/msg00005.html>
* UBUNTU: USN-903-1
<http://www.ubuntu.com/usn/USN-903-1>
* CERT: TA09-294A
<http://www.us-cert.gov/cas/techalerts/TA09-294A.html>
* CERT: TA10-159B
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
* CERT-VN: VU#466161
<http://www.kb.cert.org/vuls/id/466161>
* BID: 35671
<http://www.securityfocus.com/bid/35671>
* OSVDB: 55895
<http://osvdb.org/55895>
* OSVDB: 55907
<http://osvdb.org/55907>
* SECTRAK: 1022561
<http://www.securitytracker.com/id?1022561>
* SECTRAK: 1022567
<http://www.securitytracker.com/id?1022567>
* SECTRAK: 1022661
<http://www.securitytracker.com/id?1022661>
* SECUNIA: 35776
<http://secunia.com/advisories/35776>
* SECUNIA: 35853
<http://secunia.com/advisories/35853>
* SECUNIA: 35854
<http://secunia.com/advisories/35854>

* SECUNIA: 35855
<http://secunia.com/advisories/35855>
* SECUNIA: 35858
<http://secunia.com/advisories/35858>
* SECUNIA: 36162
<http://secunia.com/advisories/36162>
* SECUNIA: 36176
<http://secunia.com/advisories/36176>
* SECUNIA: 36180
<http://secunia.com/advisories/36180>
* SECUNIA: 35852
<http://secunia.com/advisories/35852>
* SECUNIA: 36494
<http://secunia.com/advisories/36494>
* SECUNIA: 37300
<http://secunia.com/advisories/37300>
* SECUNIA: 37671
<http://secunia.com/advisories/37671>
* SECUNIA: 37841
<http://secunia.com/advisories/37841>
* SECUNIA: 38567
<http://secunia.com/advisories/38567>
* SECUNIA: 38568
<http://secunia.com/advisories/38568>
* SECUNIA: 38695
<http://secunia.com/advisories/38695>
* SECUNIA: 38921
<http://secunia.com/advisories/38921>
* VUPEN: ADV-2009-1900
<http://www.vupen.com/english/advisories/2009/1900>
* VUPEN: ADV-2009-1908
<http://www.vupen.com/english/advisories/2009/1908>
* VUPEN: ADV-2009-1911
<http://www.vupen.com/english/advisories/2009/1911>
* VUPEN: ADV-2009-1909
<http://www.vupen.com/english/advisories/2009/1909>
* VUPEN: ADV-2009-2543
<http://www.vupen.com/english/advisories/2009/2543>
* VUPEN: ADV-2009-3122
<http://www.vupen.com/english/advisories/2009/3122>
* VUPEN: ADV-2010-0366
<http://www.vupen.com/english/advisories/2010/0366>
* VUPEN: ADV-2010-0635
<http://www.vupen.com/english/advisories/2010/0635>

CVE Reference:

CVE-2009-0217 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-1632 Apache CVSS 2.0 Score = 7.5

Apache Axis2 before 1.5.2, as used in IBM WebSphere Application Server (WAS) 7.0 through 7.0.0.12, IBM Feature Pack for Web Services 6.1.0.9 through 6.1.0.32, IBM Feature Pack for Web 2.0 1.0.1.0, Apache Synapse, Apache ODE, Apache Tuscany, Apache Geronimo, and other products, does not properly reject DTDs in SOAP messages, which allows remote attackers to read arbitrary files, send HTTP requests to intranet servers, or cause a denial of service (CPU and memory consumption) via a crafted DTD, as demonstrated by an entity declaration in a request to the Synapse SimpleStockQuoteService.

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

References:

CONFIRM: <https://svn.apache.org/repos/asf/axis/axis2/java/core/security/CVE-2010-1632.pdf>

CONFIRM: <https://issues.apache.org/jira/browse/AXIS2-4450>

VUPEN: <http://www.vupen.com/english/advisories/2010/1531>

VUPEN: <http://www.vupen.com/english/advisories/2010/1528>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21433581>

SECUNIA: <http://secunia.com/advisories/40279>

SECUNIA: <http://secunia.com/advisories/40252>

MISC: <http://markmail.org/message/e4yij7lfexastv>

CVE Reference: [CVE-2010-1632](#)

• **CVE-2010-2225 PHP CVSS 2.0 Score = 7.5**

Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.

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

References:

MISC: https://bugzilla.redhat.com/show_bug.cgi?id=605641

XF: <http://xforce.iss.net/xforce/xfdb/59610>

BID: <http://www.securityfocus.com/bid/40948>

MISC: <http://twitter.com/i0n1c/statuses/16447867829>

MISC: <http://twitter.com/i0n1c/statuses/16373156076>

MISC: <http://pastebin.com/mXGidCsd>

CVE Reference: [CVE-2010-2225](#)

• **CVE-2010-2351 Novell CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in the CIFS.NLM driver in Netware SMB 1.0 for Novell Network 6.5 SP8 and earlier allows remote attackers to execute arbitrary code via a Sessions Setup AndX packet with a long AccountName.

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

References:

CONFIRM: <http://download.novell.com/Download?buildid=tMWCI1cdl7s~>

XF: <http://xforce.iss.net/xforce/xfdb/59501>

VUPEN: <http://www.vupen.com/english/advisories/2010/1514>

MISC: <http://www.stratsec.net/Research/Advisories/SS-2010-006-Netware-SMB-Remote-Stack-Overflow>

BID: <http://www.securityfocus.com/bid/40908>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/13906>

SECUNIA: <http://secunia.com/advisories/40199>

CVE Reference: [CVE-2010-2351](#)

• **CVE-2010-0183 Mozilla CVSS 2.0 Score = 9.3**

Use-after-free vulnerability in the nsCycleCollector::MarkRoots function in Mozilla Firefox 3.5.x before 3.5.10 and SeaMonkey before 2.0.5 allows remote attackers to execute arbitrary code via a crafted HTML document, related to an improper frame construction process for menus.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=557174

BID: <http://www.securityfocus.com/bid/41050>

CONFIRM: <http://www.mozilla.org/security/announce/2010/mfsa2010-27.html>

CVE Reference: [CVE-2010-0183](#)

• **CVE-2010-1196 Mozilla CVSS 2.0 Score = 9.3**

Integer overflow in the nsGenericDOMDataNode::SetTextInternal function in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, Thunderbird before 3.0.5, and SeaMonkey before 2.0.5 allows remote attackers to execute arbitrary code via a DOM node with a long text value that triggers a heap-based buffer overflow.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=534666

BID: <http://www.securityfocus.com/bid/41050>

CONFIRM: <http://www.mozilla.org/security/announce/2010/mfsa2010-29.html>

CVE Reference: [CVE-2010-1196](#)

• **CVE-2010-1198 Mozilla CVSS 2.0 Score = 9.3**

Use-after-free vulnerability in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, and SeaMonkey before 2.0.5, allows remote attackers to execute arbitrary code via vectors involving multiple plugin instances.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=532246

BID: <http://www.securityfocus.com/bid/41050>

CONFIRM: <http://www.mozilla.org/security/announce/2010/mfsa2010-28.html>

CVE Reference: [CVE-2010-1198](#)

• **CVE-2010-1199 Mozilla CVSS 2.0 Score = 9.3**

Integer overflow in the XSLT node sorting implementation in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, Thunderbird before 3.0.5, and SeaMonkey before 2.0.5 allows remote attackers to execute arbitrary code via a large text value for a node.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=554255

BID: <http://www.securityfocus.com/bid/41050>

CONFIRM: <http://www.mozilla.org/security/announce/2010/mfsa2010-30.html>

CVE Reference: [CVE-2010-1199](#)

• **CVE-2010-1200 Mozilla CVSS 2.0 Score = 9.3**

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, Thunderbird before 3.0.5, and SeaMonkey before 2.0.5 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=553938

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=551661

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=551233

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=534768

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=531176

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=509839

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=484890

BID: <http://www.securityfocus.com/bid/41050>

CONFIRM: <http://www.mozilla.org/security/announce/2010/mfsa2010-26.html>

CVE Reference: [CVE-2010-1200](#)

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