

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

Police meet on cyber crime. Largest sentence for cyber crime. New type of malware overwrites software update. Report about the malware sources.

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

• Police, security officials meet on cybercrime strategies

IDG News Service - When the "ILOVEYOU" worm crippled computer systems worldwide 10 years ago this spring, authorities in the Philippines didn't even have a law to properly charge its author.

Since that time, many countries have developed computer crime laws in part due to the 2001 Convention on Cybercrime, an international treaty that lays out legal guidelines for high-tech crime legislation.

This week, more than 300 experts met at the Council of Europe's conference on cybercrime to discuss the treaty and better cooperation in a fast-changing landscape where criminals clearly still have the upper hand. Computerworld

Full Story :

http://www.computerworld.com/s/article/9174102/Police_security_officials_meet_on_cybercrime_strategies?source=

• Hacker Albert Gonzalez receives 20 years in prison

Albert Gonzalez on Thursday received the largest-ever U.S. prison sentence for a hacker. Gonzalez, 28, of Miami, was sentenced to 20 years in prison for leading a group of cybercriminals that stole tens of millions of credit and debit card numbers from TJX and several other retailers.

Gonzalez pleaded guilty in September to multiple federal charges of conspiracy, computer fraud, access device fraud and identity theft for hacking into TJX, which owns T.J. Maxx, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble and Sports Authority. He was facing up to 25 years in prison for these charges.

Gonzalez also pleaded guilty last year in two other pending hacking cases for which he is scheduled to be sentenced on Friday. He faces up to 20 years in prison for his role in hacking into the network of Dave & Buster's restaurant chain and stealing credit and debit card numbers from at least 11 locations. SC Magazine

Full Story :

http://www.scmagazineus.com/hacker-albert-gonzalez-receives-20-years-in-prison/article/166571/?utm_source=feed

• New malware overwrites software updaters

IDG News Service - For the first time security researchers have spotted a type of malicious software that overwrites update functions for other applications, which could pose additional long-term risks for users.

The malware, which infects Windows computers, masks itself as an updater for Adobe Systems' products and other software such as Java, wrote Nguyen Cong Cuong, an analyst with Bach Khoa Internetwork Security (BKIS), a Vietnamese security company, on its blog.

BKIS showed screen shots of a variant of the malware that imitates Adobe Reader version 9 and overwrites the AdobeUpdater.exe, which regularly checks in with Adobe to see if a new version of the software is available. Computerworld

Full Story :

http://www.computerworld.com/s/article/9174126/New_malware_overwrites_software_updaters?source=rss_security

• Symantec finds China top source of malware

More malware is now coming out of China than from any other country, according to a new report from Symantec.

The United States still leads the world in the number of malware attacks sent from mail servers. Symantec's report (PDF) found U.S. mail servers responsible for distributing 36.6 percent of all global malware in March, followed by China at 17.8 percent and Romania at 16.5 percent.

Symantec captured these results by analyzing the IP addresses of sending mail servers. The company uncovered a large amount of malware from the United States in large part because many Web-based e-mail services, such as Gmail and Yahoo Mail, are hosted in the U.S. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20001234-83.html?part=rss&subj=news&tag=2547-1_3-0-20

• Taxpayer data at risk from IRS security flaws

The Internal Revenue Service's failure to use strong passwords, install patches quickly, and adequately control access to computer systems and information makes the system vulnerable to insider threats and attacks from outside, a new government report concludes.

The IRS has failed to fix almost 70 percent of control weaknesses and program deficiencies identified a year ago, the Government Accountability Office said in a report released last week.

Specifically, the IRS has corrected or mitigated 28 of 89 weaknesses and deficiencies found, but left 61 of them unresolved, according to the report. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20000987-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 18731 Wireshark Paltalk dissector Denial of Service Vulnerability (Remote File Checking)

packet-paltalk.c in the Paltalk dissector in Wireshark 1.2.0 through 1.2.2, on SPARC and certain other platforms, allows remote attackers to cause a denial of service (application crash) via a file that records a malformed packet trace.

The vulnerability is reported in versions 1.2.0 to 1.2.2.

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

References:

- * CONFIRM:
<http://www.wireshark.org/docs/relnotes/wireshark-1.2.3.html>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-07.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=3689
- * BID: 36846
<http://www.securityfocus.com/bid/36846>
- * SECUNIA: 37175
<http://secunia.com/advisories/37175>
- * SECUNIA: 37409
<http://secunia.com/advisories/37409>
- * VUPEN: ADV-2009-3061
<http://www.vupen.com/english/advisories/2009/3061>
- * XF: wireshark-dissectpaltalk-dos(54016)
<http://xforce.iss.net/xforce/xfdb/54016>

CVE Reference:

CVE-2009-3549 (cve.mitre.org, nvd.nist.gov)

• 18732 Wireshark DCERPC/NT dissector Denial of Service Vulnerability (Remote File Checking)

The DCERPC/NT dissector in Wireshark 0.10.10 through 1.0.9 and 1.2.0 through 1.2.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a file that records a malformed packet trace. NOTE: some of these details are obtained from third party information.

The vulnerability is reported in versions 0.10.10 to 1.0.9, 1.2.0 to 1.2.2.

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

References:

- * CONFIRM:
<http://www.wireshark.org/docs/relnotes/wireshark-1.0.10.html>
- * CONFIRM:
<http://www.wireshark.org/docs/relnotes/wireshark-1.2.3.html>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-07.html>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-08.html>
- * DEBIAN: DSA-1942
<http://www.debian.org/security/2009/dsa-1942>
- * BID: 36846
<http://www.securityfocus.com/bid/36846>
- * SECUNIA: 37175
<http://secunia.com/advisories/37175>
- * SECUNIA: 37409
<http://secunia.com/advisories/37409>
- * SECUNIA: 37477
<http://secunia.com/advisories/37477>
- * VUPEN: ADV-2009-3061
<http://www.vupen.com/english/advisories/2009/3061>
- * XF: wireshark-dcerpcnt-dos(54017)
<http://xforce.iss.net/xforce/xfdb/54017>

CVE Reference:

CVE-2009-3550 (cve.mitre.org, nvd.nist.gov)

• 18733 Wireshark SMB dissector Denial of Service Vulnerability (CVE-2009-3551) (Remote File Checking)

Off-by-one error in the dissect_negprot_response function in packet-smb.c in the SMB dissector in Wireshark 1.2.0 through 1.2.2 allows remote attackers to cause a denial of service (application crash) via a file that records a malformed packet trace. NOTE: some of these details are obtained from third party information.

The vulnerability is reported in versions 1.2.0 to 1.2.2.

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

References:

- * CONFIRM:
<http://www.wireshark.org/docs/relnotes/wireshark-1.2.3.html>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-07.html>
- * BID: 36846
<http://www.securityfocus.com/bid/36846>
- * SECUNIA: 37175
<http://secunia.com/advisories/37175>
- * SECUNIA: 37409
<http://secunia.com/advisories/37409>
- * VUPEN: ADV-2009-3061
<http://www.vupen.com/english/advisories/2009/3061>
- * XF: wireshark-negprotresponse-dos(54018)
<http://xforce.iss.net/xforce/xfdb/54018>

CVE Reference:

CVE-2009-3551 (cve.mitre.org, nvd.nist.gov)

• 18734 Wireshark Daintree SNA dissector buffer overflow Vulnerability (Remote File Checking)

Buffer overflow in the daintree_sna_read function in the Daintree SNA file parser in Wireshark 1.2.0 through 1.2.4 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet.

The vulnerability is reported in versions 1.2.0 to 1.2.4.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack / Crash** Risk: **High**

References:

- * MISC:
<https://bugs.wireshark.org/bugzilla/attachment.cgi?id=4022>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-09.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4294
- * FEDORA: FEDORA-2009-13592
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01248.html>
- * BID: 37407
<http://www.securityfocus.com/bid/37407>
- * OSVDB: 61177
<http://osvdb.org/61177>
- * SECTRAK: 1023374
<http://www.securitytracker.com/id?1023374>
- * SECUNIA: 37842
<http://secunia.com/advisories/37842>
- * SECUNIA: 37916
<http://secunia.com/advisories/37916>
- * VUPEN: ADV-2009-3596
<http://www.vupen.com/english/advisories/2009/3596>

CVE Reference:

CVE-2009-4376 (cve.mitre.org, nvd.nist.gov)

• 18735 Wireshark SMB and SMB2 dissectors Denial of Service Vulnerability (Remote File Checking)

The (1) SMB and (2) SMB2 dissectors in Wireshark 0.9.0 through 1.2.4 allow remote attackers to cause a denial of service (crash) via a crafted packet that triggers a NULL pointer dereference, as demonstrated by fuzz-2009-12-07-11141.pcap.

The vulnerability is reported in versions 0.9.0 to 1.0.10, 1.2.0 to 1.2.4.

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

References:

- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-09.html>

* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4301
* DEBIAN: DSA-1983
<http://www.debian.org/security/2009/dsa-1983>
* FEDORA: FEDORA-2009-13592
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01248.html>
* MANDRIVA: MDVSA-2010:031
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:031>
* BID: 37407
<http://www.securityfocus.com/bid/37407>
* OSVDB: 61178
<http://osvdb.org/61178>
* SECTrack: 1023374
<http://www.securitytracker.com/id?1023374>
* SECUNIA: 37842
<http://secunia.com/advisories/37842>
* SECUNIA: 37916
<http://secunia.com/advisories/37916>
* VUPEN: ADV-2009-3596
<http://www.vupen.com/english/advisories/2009/3596>

CVE Reference:

CVE-2009-4377 (cve.mitre.org, nvd.nist.gov)

• 18736 Wireshark IPMI dissector Denial of Service Vulnerability (Remote File Checking)

The IPMI dissector in Wireshark 1.2.0 through 1.2.4, when running on Windows, allows remote attackers to cause a denial of service (crash) via a crafted packet, related to "formatting a date/time using strftime."

The vulnerability is reported in versions 1.2.0 to 1.2.4.

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

References:

* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-09.html>
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=4301
* FEDORA: FEDORA-2009-13592
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01248.html>
* BID: 37407
<http://www.securityfocus.com/bid/37407>
* OSVDB: 61179
<http://osvdb.org/61179>
* SECTrack: 1023374
<http://www.securitytracker.com/id?1023374>
* SECUNIA: 37842
<http://secunia.com/advisories/37842>
* VUPEN: ADV-2009-3596
<http://www.vupen.com/english/advisories/2009/3596>

CVE Reference:

CVE-2009-4378 (cve.mitre.org, nvd.nist.gov)

• 18737 Wireshark LWRES dissector buffer overflow Vulnerabilities (Remote File Checking)

Multiple buffer overflows in the LWRES dissector in Wireshark 0.9.15 through 1.0.10 and 1.2.0 through 1.2.5 allow remote attackers to cause a denial of service (crash) via a malformed packet, as demonstrated using a stack-based buffer overflow to the dissect_getaddrsbyname_request function.

The vulnerability is reported in versions 0.9.15 to 1.0.10, 1.2.0 to 1.2.5.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack / Crash** Risk: **High**

References:

* MLIST: [oss-security] 20100129 Re: CVE id request: Wireshark
<http://www.openwall.com/lists/oss-security/2010/01/29/4>
* MISC:
<http://anonsvn.wireshark.org/viewvc/trunk-1.2/epan/dissectors/packet-lwres.c?view=diff&r1=31596&r2=28492&diff=1>

* MISC:

http://www.metasploit.com/modules/exploit/multi/misc/wireshark_lwres_getaddrbyname

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2010-02.html>

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2010-01.html>

* DEBIAN: DSA-1983

<http://www.debian.org/security/2010/dsa-1983>

* MANDRIVA: MDVSA-2010:031

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:031>

* BID: 37985

<http://www.securityfocus.com/bid/37985>

* OSVDB: 61987

<http://osvdb.org/61987>

* SECTRAK: 1023516

<http://www.securitytracker.com/id?1023516>

* SECUNIA: 38257

<http://secunia.com/advisories/38257>

* SECUNIA: 38348

<http://secunia.com/advisories/38348>

* VUPEN: ADV-2010-0239

<http://www.vupen.com/english/advisories/2010/0239>

* XF: wireshark-lwres-bo(55951)

<http://xforce.iss.net/xforce/xfdb/55951>

CVE Reference:

CVE-2010-0304 (cve.mitre.org, nvd.nist.gov)

• 18738 Apache Tomcat Unexpected file deletion in work directory Vulnerability

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

When deploying WAR files, the WAR file names were not checked for directory traversal attempts. For example, deploying and undeploying ...war allows an attacker to cause the deletion of the current contents of the host's work directory which may cause problems for currently running applications.

The issue has been addressed in Apache Tomcat version 6.0.24, 5.5.29.

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

References:

* BUGTRAQ: 20100124 [SECURITY] CVE-2009-2902 Apache Tomcat unexpected file deletion in work directory

<http://www.securityfocus.com/archive/1/archive/1/509150/100/0/threaded>

* CONFIRM:

<http://svn.apache.org/viewvc?rev=892815&view=rev>

* CONFIRM:

<http://svn.apache.org/viewvc?rev=902650&view=rev>

* CONFIRM:

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

* CONFIRM:

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

* UBUNTU: USN-899-1

<http://ubuntu.com/usn/usn-899-1>

* BID: 37945

<http://www.securityfocus.com/bid/37945>

* SECTRAK: 1023504

<http://securitytracker.com/id?1023504>

* SECUNIA: 38316

<http://secunia.com/advisories/38316>

* SECUNIA: 38346

<http://secunia.com/advisories/38346>

* SECUNIA: 38541

<http://secunia.com/advisories/38541>

* VUPEN: ADV-2010-0213

<http://www.vupen.com/english/advisories/2010/0213>

* XF: apache-tomcat-war-directory-traversal(55857)

<http://xforce.iss.net/xforce/xfdb/55857>

CVE Reference:

CVE-2009-2902 (cve.mitre.org, nvd.nist.gov)

• **18739 Apache Tomcat Insecure partial deploy after failed deploy Vulnerability**

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

The autodeployment process in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20, when autoDeploy is enabled, deploys appBase files that remain from a failed undeploy, which might allow remote attackers to bypass intended authentication requirements via HTTP requests.

The issue has been addressed in Apache Tomcat version 6.0.24, 5.5.29.

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

References:

- * BUGTRAQ: 20100124 [SECURITY] CVE-2009-2901 Apache Tomcat insecure partial deploy after failed undeploy
<http://www.securityfocus.com/archive/1/archive/1/509151/100/0/threaded>
- * CONFIRM:
<http://svn.apache.org/viewvc?rev=892815&view=rev>
- * CONFIRM:
<http://svn.apache.org/viewvc?rev=902650&view=rev>
- * CONFIRM:
<http://tomcat.apache.org/security-5.html>
- * CONFIRM:
<http://tomcat.apache.org/security-6.html>
- * UBUNTU: USN-899-1
<http://ubuntu.com/usn/usn-899-1>
- * BID: 37942
<http://www.securityfocus.com/bid/37942>
- * SECTRAK: 1023503
<http://securitytracker.com/id?1023503>
- * SECUNIA: 38316
<http://secunia.com/advisories/38316>
- * SECUNIA: 38346
<http://secunia.com/advisories/38346>
- * SECUNIA: 38541
<http://secunia.com/advisories/38541>
- * VUPEN: ADV-2010-0213
<http://www.vupen.com/english/advisories/2010/0213>
- * XF: tomcat-autodeploy-security-bypass(55856)
<http://xforce.iss.net/xforce/xfdb/55856>

CVE Reference:

CVE-2009-2901 (cve.mitre.org, nvd.nist.gov)

• **18740 Apache Tomcat Arbitrary file deletion and/or alteration on deploy Vulnerability**

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

Directory traversal vulnerability in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20 allows remote attackers to create or overwrite arbitrary files via a .. (dot dot) in an entry in a WAR file, as demonstrated by a ../../bin/catalina.bat entry.

The issue has been addressed in Apache Tomcat version 6.0.24, 5.5.29.

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

References:

- * BUGTRAQ: 20100124 [SECURITY] CVE-2009-2693 Apache Tomcat unexpected file deletion and/or alteration
<http://www.securityfocus.com/archive/1/archive/1/509148/100/0/threaded>
- * CONFIRM:
<http://svn.apache.org/viewvc?rev=892815&view=rev>
- * CONFIRM:
<http://svn.apache.org/viewvc?rev=902650&view=rev>
- * CONFIRM:
<http://tomcat.apache.org/security-5.html>
- * CONFIRM:
<http://tomcat.apache.org/security-6.html>
- * UBUNTU: USN-899-1
<http://ubuntu.com/usn/usn-899-1>

* BID: 37944
<http://www.securityfocus.com/bid/37944>
* SECTrack: 1023505
<http://securitytracker.com/id?1023505>
* SECUNIA: 38316
<http://secunia.com/advisories/38316>
* SECUNIA: 38346
<http://secunia.com/advisories/38346>
* SECUNIA: 38541
<http://secunia.com/advisories/38541>
* VUPEN: ADV-2010-0213
<http://www.vupen.com/english/advisories/2010/0213>
* XF: tomcat-war-directory-traversal(55855)
<http://xforce.iss.net/xforce/xfdb/55855>

CVE Reference:

CVE-2009-2693 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-1098 Microsoft CVSS 2.0 Score = 7.1

The ANI parser in Microsoft Windows before 7 on the x86 platform, as used in Internet Explorer and other applications, allows remote attackers to cause a denial of service (memory and CPU consumption) via a crafted biClrUsed value in the BITMAPINFO header of a .ANI file.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56756>

BID: <http://www.securityfocus.com/bid/38579>

MISC: <http://skypher.com/index.php/2010/03/08/ani-file-bitmapinfoheader-biclrused-bounds-check-missing/>

MISC: <http://code.google.com/p/skylined/issues/detail?id=3>

CVE Reference: [CVE-2010-1098](#)

• CVE-2010-1042 Microsoft CVSS 2.0 Score = 4.3

Microsoft Windows Media Player 11 does not properly perform colorspace conversion, which allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted .AVI file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.

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

References:

BID: <http://www.securityfocus.com/bid/38790>

CVE Reference: [CVE-2010-1042](#)

• CVE-2010-1041 IBM CVSS 2.0 Score = 10.0

Unspecified vulnerability in the single sign-on functionality in the Web Services implementation in IBM DB2 Content Manager (CM) Toolkit 8.3 before FP13 on z/OS and DB2 Information Integrator for Content 8.3 before FP13 has unknown impact and remote attack vectors.

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

References:

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=isg1PM03804>

VUPEN: <http://www.vupen.com/english/advisories/2010/0656>

BID: <http://www.securityfocus.com/bid/38833>

OSVDB: <http://www.osvdb.org/63079>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27018205&aid=1>

SECTrack: <http://securitytracker.com/id?1023726>

SECUNIA: <http://secunia.com/advisories/39025>

CVE Reference: [CVE-2010-1041](#)

• **CVE-2010-0437 Linux CVSS 2.0 Score = 7.8**

The ip6_dst_lookup_tail function in net/ipv6/ip6_output.c in the Linux kernel before 2.6.27 does not properly handle certain circumstances involving an IPv6 TUN network interface and a large number of neighbors, which allows attackers to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via unknown vectors.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=563781

MLIST: <http://www.openwall.com/lists/oss-security/2010/03/04/4>

MLIST: <http://www.openwall.com/lists/oss-security/2010/02/11/1>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.27>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=e550dfb0c2c31b6363aa463a035fc9f8dcaa3c9b>

CONFIRM: http://bugzilla.kernel.org/show_bug.cgi?id=11469

CVE Reference: [CVE-2010-0437](#)

• **CVE-2009-3385 Mozilla CVSS 2.0 Score = 7.1**

The mail component in Mozilla SeaMonkey before 1.1.19 does not properly restrict execution of scriptable plugin content, which allows user-assisted remote attackers to obtain sensitive information via crafted content in an IFRAME element in an HTML e-mail message, as demonstrated by a Flash object that sends arbitrary local files during a reply or forward operation.

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

References:

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

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=371976

BID: <http://www.securityfocus.com/bid/38830>

CONFIRM: <http://www.mozilla.org/security/announce/2010/mfsa2010-06.html>

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

CVE Reference: [CVE-2009-3385](#)

• **CVE-2010-1099 Apple CVSS 2.0 Score = 5.0**

Integer overflow in Apple Safari allows remote attackers to bypass intended port restrictions on outbound TCP connections via a port number outside the range of the unsigned short data type, as demonstrated by a value of 65561 for TCP port 25.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/510283/100/0/threaded>

CVE Reference: [CVE-2010-1099](#)

• **CVE-2010-0163 Mozilla CVSS 2.0 Score = 4.3**

Mozilla Thunderbird before 2.0.0.24 and SeaMonkey before 1.1.19 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.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=505221

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

XF: <http://xforce.iss.net/xforce/xfdb/56993>

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

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

BID: <http://www.securityfocus.com/bid/38831>

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

CVE Reference: [CVE-2010-0163](#)

• CVE-2010-0161 Mozilla CVSS 2.0 Score = 4.3

The nsAuthSSPI::Unwrap function in extensions/auth/nsAuthSSPI.cpp in Mozilla Thunderbird before 2.0.0.24 and SeaMonkey before 1.1.19 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.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=511806

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

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

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

BID: <http://www.securityfocus.com/bid/38831>

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

CVE Reference: [CVE-2010-0161](#)

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