

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

New plan for cyber security on the way. Kraken botnet live again. Microsoft warns of exploit. Third-party apps don't use security features available.

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

- **White House drafting plan for cyberspace safety**

Got an idea for improving cybersecurity?

(Credit: Department of Homeland Security) The White House is hoping to come up with a comprehensive strategy to better protect people in cyberspace and is asking the public for help.

Releasing a draft of the potential new National Strategy for Trusted Identities in Cyberspace (PDF) last Friday, the government is aiming to set up a system that would let people voluntarily create trusted identities to use in online transactions. Cnet Security

Full Story :

http://news.cnet.com/8301-13578_3-20008998-38.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Kraken botnet re-emerges 318,000 nodes strong**

Kraken, a large and difficult-to-detect botnet that peaked in 2008 and was dismantled by early 2009, is back, and anti-virus solutions are struggling to detect it, according to researchers at Georgia Tech Information Security Center.

The botnet reappeared in April and, as of last week, was made up of more than 318,000 unique IP addresses, or about half its 650,000 maximum size in 2008, Paul Royal, research scientist at the Georgia Tech center told SCMagazineUS.com on Wednesday.

Machines infected by Kraken malware primarily are being used to send spam, and a single member of the botnet is capable of sending more than 600,000 unwanted emails in a 24-hour period, he said. All of the spam is promoting male enhancement or erectile dysfunction products. SC Magazine

Full Story :

http://www.scmagazineus.com/kraken-botnet-re-emerges-318000-nodes-strong/article/173611/?utm_source=feedbur

• Microsoft warns of soaring Windows Help Center exploits

Attacks taking advantage of a zero-day Windows Help and Support Center vulnerability drastically have gained in prevalence and scope in recent days, malware specialists at Microsoft warned Thursday evening.

Holly Stewart, a senior program manager with the Microsoft Malware Protection Center, said engineers began spotting in-the-wild exploits targeting the flaw on June 15, five days after the software giant confirmed the bug with the release of a security advisory. The vulnerability, which affects Windows XP and Server 2003 machines, was discovered by Google engineer Tavis Ormandy, who published exploit code in a post on the Full Disclosure mailing list.

Ormandy's disclosure prompted a number of other proof-of-concepts, followed by active exploits that initially were "targeted and fairly limited" in nature, Stewart said. However, recently the scope of the attacks dramatically has widened. SC Magazine

Full Story :

http://www.scmagazineus.com/microsoft-warns-of-soaring-windows-help-center-exploits/article/173739/?utm_source

• Third-party apps failing to use Windows security features

Many third-party Windows applications are failing to utilize two important security features that could prevent certain code execution attacks, according to a report released Thursday by Secunia.

Researchers at the Danish vulnerability tracking firm recently investigated whether some of the most popular third-party applications used two built-in Windows security features, known as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).

DEP, first introduced in the Windows XP Service Pack 2 in August 2004, makes part of the memory nonexecutable and, as a result, renders the exploit development process more complex and time consuming. SC Magazine

Full Story :

http://www.scmagazineus.com/third-party-apps-failing-to-use-windows-security-features/article/173746/?utm_source

New Vulnerabilities Tested in SecureScout

• 14564 Adobe Acrobat / Reader Cross-site scripting Vulnerability (CVE-2010-0190) (Remote File Checking)

Cross-site scripting (XSS) vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-09.html>

* CERT: TA10-103C

<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>

* BID: 39329

<http://www.securityfocus.com/bid/39329>

* VUPEN: ADV-2010-0873

<http://www.vupen.com/english/advisories/2010/0873>

CVE Reference:

CVE-2010-0190 (cve.mitre.org, nvd.nist.gov)

● **14565 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0191) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified vectors, related to a "prefix protocol handler vulnerability."

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>
- * CERT: TA10-103C
<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>
- * BID: 39329
<http://www.securityfocus.com/bid/39329>
- * VUPEN: ADV-2010-0873
<http://www.vupen.com/english/advisories/2010/0873>

CVE Reference:

CVE-2010-0191 (cve.mitre.org, nvd.nist.gov)

● **14566 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0192) (Remote File Checking)**

Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2010-0193 and CVE-2010-0196.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>
- * CERT: TA10-103C
<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>
- * BID: 39329
<http://www.securityfocus.com/bid/39329>
- * VUPEN: ADV-2010-0873
<http://www.vupen.com/english/advisories/2010/0873>

CVE Reference:

CVE-2010-0192 (cve.mitre.org, nvd.nist.gov)

● **14567 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0193) (Remote File Checking)**

Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2010-0192 and CVE-2010-0196.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>
- * CERT: TA10-103C
<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>
- * BID: 39329
<http://www.securityfocus.com/bid/39329>
- * VUPEN: ADV-2010-0873
<http://www.vupen.com/english/advisories/2010/0873>
- * XF: adobe-acrobat-unspec-code-exec(57701)
<http://xforce.iss.net/xforce/xfdb/57701>

CVE Reference:

CVE-2010-0193 (cve.mitre.org, nvd.nist.gov)

● **14568 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0194) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0197, CVE-2010-0201, and CVE-2010-0204.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>
- * CERT: TA10-103C
<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>
- * BID: 39329
<http://www.securityfocus.com/bid/39329>
- * VUPEN: ADV-2010-0873
<http://www.vupen.com/english/advisories/2010/0873>

CVE Reference:

CVE-2010-0194 (cve.mitre.org, nvd.nist.gov)

• **14569 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0195) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, do not properly handle fonts, which allows attackers to execute arbitrary code via unspecified vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>
- * CERT: TA10-103C
<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>
- * BID: 39329
<http://www.securityfocus.com/bid/39329>
- * VUPEN: ADV-2010-0873
<http://www.vupen.com/english/advisories/2010/0873>

CVE Reference:

CVE-2010-0195 (cve.mitre.org, nvd.nist.gov)

• **14570 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0196) (Remote File Checking)**

Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2010-0192 and CVE-2010-0193.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>
- * CERT: TA10-103C
<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>
- * BID: 39329
<http://www.securityfocus.com/bid/39329>
- * VUPEN: ADV-2010-0873
<http://www.vupen.com/english/advisories/2010/0873>

CVE Reference:

CVE-2010-0196 (cve.mitre.org, nvd.nist.gov)

• **14571 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0197) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0194, CVE-2010-0201, and CVE-2010-0204.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>
- * CERT: TA10-103C
<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>
- * BID: 39329
<http://www.securityfocus.com/bid/39329>
- * VUPEN: ADV-2010-0873
<http://www.vupen.com/english/advisories/2010/0873>

CVE Reference:

CVE-2010-0197 (cve.mitre.org, nvd.nist.gov)

• 14572 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0198) (Remote File Checking)

Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0199, CVE-2010-0202, and CVE-2010-0203.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>
- * CERT: TA10-103C
<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>
- * BID: 39329
<http://www.securityfocus.com/bid/39329>
- * VUPEN: ADV-2010-0873
<http://www.vupen.com/english/advisories/2010/0873>

CVE Reference:

CVE-2010-0198 (cve.mitre.org, nvd.nist.gov)

• 14573 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0199) (Remote File Checking)

Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0198, CVE-2010-0202, and CVE-2010-0203.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>
- * CERT: TA10-103C
<http://www.us-cert.gov/cas/techalerts/TA10-103C.html>
- * BID: 39329
<http://www.securityfocus.com/bid/39329>
- * VUPEN: ADV-2010-0873
<http://www.vupen.com/english/advisories/2010/0873>

CVE Reference:

CVE-2010-0199 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-2517 IBM CVSS 2.0 Score = 7.5

Multiple unspecified vulnerabilities in IBM Rational ClearQuest before 7.1.1.02 have unknown impact and attack vectors, as demonstrated by an AppScan report.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/1615>

BID: <http://www.securityfocus.com/bid/41205>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM07157>

SECUNIA: <http://secunia.com/advisories/40341>

CVE Reference: [CVE-2010-2517](#)

• CVE-2010-2518 IBM CVSS 2.0 Score = 7.5

Unspecified vulnerability in the P8 Content Engine (P8CE) 4.5.1 before FP3 and the P8 Content Search Engine (P8CSE) before 4.5.0 FP3 and 4.5.1 before FP1, as used in IBM FileNet P8 Content Manager (CM) and FileNet P8 Business Process Manager (BPM), allows remote attackers to gain privileges via unknown vectors. NOTE: some of these details are obtained from third party information.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/59792>

VUPEN: <http://www.vupen.com/english/advisories/2010/1616>

BID: <http://www.securityfocus.com/bid/41177>

OSVDB: <http://www.osvdb.org/65804>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21438487>

SECUNIA: <http://secunia.com/advisories/40413>

CVE Reference: [CVE-2010-2518](#)

• CVE-2009-4912 Cisco CVSS 2.0 Score = 10.0

Cisco Adaptive Security Appliances (ASA) 5580 series devices with software before 8.1(2) complete an SSL handshake with an HTTPS client even if this client is unauthorized, which might allow remote attackers to bypass intended access restrictions via an HTTPS session, aka Bug ID CSCso10876.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn812.html>

CVE Reference: [CVE-2009-4912](#)

• CVE-2009-4919 Cisco CVSS 2.0 Score = 10.0

Buffer overflow on Cisco Adaptive Security Appliances (ASA) 5580 series devices with software before 8.1(2) allows remote attackers to have an unspecified impact via long IKE attributes, aka Bug ID CSCsu43121.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn812.html>

CVE Reference: [CVE-2009-4919](#)

• CVE-2009-4911 Cisco CVSS 2.0 Score = 7.8

Unspecified vulnerability on Cisco Adaptive Security Appliances (ASA) 5580 series devices with software before 8.1(2) allows remote attackers to cause a denial of service (device crash) via vectors involving SSL VPN and PPPoE transactions, aka Bug ID CSCsm77958.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn812.html>

CVE Reference: [CVE-2009-4911](#)

• **CVE-2009-4914 Cisco CVSS 2.0 Score = 7.8**

Memory leak on Cisco Adaptive Security Appliances (ASA) 5580 series devices with software before 8.1(2) allows remote attackers to cause a denial of service (memory consumption) via Subject Alternative Name fields in an X.509 certificate, aka Bug ID CSCsq17879.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn812.html>

CVE Reference: [CVE-2009-4914](#)

• **CVE-2009-4915 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability on Cisco Adaptive Security Appliances (ASA) 5580 series devices with software before 8.1(2) allows remote attackers to cause a denial of service (device reload) via unknown network traffic, as demonstrated by a "connection stress test," aka Bug ID CSCsq68451.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn812.html>

CVE Reference: [CVE-2009-4915](#)

• **CVE-2009-4917 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability on Cisco Adaptive Security Appliances (ASA) 5580 series devices with software before 8.1(2) allows remote attackers to cause a denial of service (device reload) via a high volume of SIP traffic, aka Bug ID CSCsr65901.

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

References:

CONFIRM: <http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn812.html>

CVE Reference: [CVE-2009-4917](#)

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