

## 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

A more complete vulnerability management. Federal Cloud security missing. NSA launches new monitoring program. June hot when it comes to malware.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netvigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • Closing the loop on threats

You break out your trusty vulnerability scanner and go to work on the weekly perimeter scan. You find a couple of new vulnerabilities and you print out the scanner's report. Now what?

Usually, there are a couple of choices. First, you can remediate the vulnerabilities yourself (or with your team) and then retest to make sure the vulnerability is fixed. Then you write a new report and send it to the boss. Time spent? Probably a day or so overall, depending on how much help you've needed.

The other option is that you can open a trouble ticket, wait for the ticket to get a response, hope that the vulnerability really is fixed before the ticket closes so that you won't find that it wasn't forcing you to reopen the ticket or open another. More than a day will have elapsed on this one in most cases. SC Magazine

Full Story :

<http://www.scmagazineus.com/closing-the-loop-on-threats/article/172677/>

### • **GAO: Federal agencies lack advisement on cloud security**

A growing number of federal agencies are running some form of cloud computing, but nearly all lack policies around securing data hosted offsite, according to a new report from the U.S. Government Accountability Office (GAO).

A lack of government-wide guidance appears to be the major holdup.

"Although individual agencies have identified security measures needed when using cloud computing, they have not always developed corresponding guidance," the report, released Thursday, said. "Until federal guidance and processes that specifically address information security for cloud computing are developed, agencies may be hesitant to implement cloud computing, and those programs that have been implemented may not have effective information security controls in place." SC Magazine

Full Story :

[http://www.scmagazineus.com/gao-federal-agencies-lack-advisement-on-cloud-security/article/174041/?utm\\_source=](http://www.scmagazineus.com/gao-federal-agencies-lack-advisement-on-cloud-security/article/174041/?utm_source=)

### • **Password stealers and Conficker top June malware**

June proved to be another hot month for malware with by a surge in attacks by a password-stealing bot and the return of old nemesis Conficker, according to a report released Tuesday by security software maker Sunbelt.

Designed to ferret out cached passwords and log-in credentials for banking sites, "Trojan-Spy.Win32.Zbot.gen" was the second-most prevalent piece of malware detected by Sunbelt last month, up from the No. 5 spot in May. The top spot, grabbing more than a quarter of all detections, was held by "Trojan.Win32.Generic!BT," a generic form of malware with hundreds of variations and sometimes associated with scareware and rogue security software, noted Sunbelt.

(Credit: Sunbelt Software) Cnet Security

Full Story :

[http://news.cnet.com/8301-1009\\_3-20009730-83.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-1009_3-20009730-83.html?part=rss&subj=news&tag=2547-1_3-0-20)

### • **Report: NSA initiating program to detect cyberattacks**

The National Security Agency is reportedly launching a program to monitor for cyberattacks against government agencies and private companies responsible for key services such as electricity, nuclear power, and transportation, according to a story in Thursday's Wall Street Journal.

The program, known as "Perfect Citizen," is already triggering mixed reactions, says the Journal. Some in industry and government see it as an attempt by the NSA to intrude into domestic matters, while others believe it's a much-needed step in fighting the threat of cyberattacks.

Perfect Citizen would establish a series of sensors across various computer networks that would sound an alarm in the event of a possible cyberattack. The sensors would be deployed at agencies and private companies that handle the nation's most critical infrastructure, including the electrical grid, nuclear power plants, subway systems, and air-traffic control networks. Cnet Security

Full Story :

[http://news.cnet.com/8301-1009\\_3-20009952-83.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-1009_3-20009952-83.html?part=rss&subj=news&tag=2547-1_3-0-20)

### • **Survey: Businesses snooped on by ex-employees, IT staff**

Many IT folks think snooping is on the rise at their companies. They may know best since they're the ones doing some of the snooping, at least according to survey results released Wednesday by Cyber-Ark.

To put together its fourth annual "Trust, Security and Passwords" (PDF) survey, security vendor Cyber-Ark said it questioned more than 400 IT professionals across the U.S. and the U.K., mostly from enterprise-size businesses.

Among those surveyed, 67 percent admitted that they accessed confidential information not relevant to their jobs. In nominating the department most likely to snoop, 54 percent pointed the finger at IT due to the group's power and responsibility in maintaining multiple computer systems throughout their companies. Cnet Security

Full Story :

[http://news.cnet.com/8301-1009\\_3-20009990-83.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-1009_3-20009990-83.html?part=rss&subj=news&tag=2547-1_3-0-20)

## **New Vulnerabilities Tested in SecureScout**

### • **14574 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0201) (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-2010-0197, 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-2010-0201 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14575 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0202) (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-2010-0199, 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-2010-0202 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14576 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0203) (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-2010-0199, and CVE-2010-0202.

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-2010-0203 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14577 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-0204) (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-2010-0197, and CVE-2010-0201.

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>
- \* BID: 39522  
<http://www.securityfocus.com/bid/39522>
- \* VUPEN: ADV-2010-0873  
<http://www.vupen.com/english/advisories/2010/0873>
- \* XF: acrobat-unspec-code-execution(57711)  
<http://xforce.iss.net/xforce/xfdb/57711>

#### CVE Reference:

CVE-2010-0204 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14578 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-1241) (Remote File Checking)

Heap-based buffer overflow in the custom heap management system 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 execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDF document, aka FG-VD-10-005.

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

#### References:

- \* MLIST: [dailydave] 20100401 Oday, it may not be  
<http://lists.immunitysec.com/pipermail/dailydave/2010-April/006077.html>
- \* MISC:  
<http://blog.fortinet.com/the-upcoming-blackhat-europe-2010-presentation/>
- \* MISC:  
<http://www.blackhat.com/html/bh-eu-10/bh-eu-10-briefings.html#Li>
- \* MISC:  
<http://www.youtube.com/watch?v=9EVHtY1-0q8>
- \* 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: 39227  
<http://www.securityfocus.com/bid/39227>
- \* BID: 39329  
<http://www.securityfocus.com/bid/39329>
- \* VUPEN: ADV-2010-0873  
<http://www.vupen.com/english/advisories/2010/0873>
- \* XF: reader-customheap-code-execution(57589)  
<http://xforce.iss.net/xforce/xfdb/57589>

#### CVE Reference:

CVE-2010-1241 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 14579 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-1240) (Remote File Checking)

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, do not restrict the contents of one text field in the Launch File warning dialog, which makes it easier for remote attackers to trick users into executing an arbitrary local program that was specified in a PDF document, as demonstrated by a text field that claims that the Open button will enable the user to read an encrypted message.

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

#### References:

- \* MLIST: [dailydave] 20100401 Oday, it may not be  
<http://lists.immunitysec.com/pipermail/dailydave/2010-April/006075.html>
- \* MISC:  
<http://blog.didierstevens.com/2010/03/29/escape-from-pdf/>

\* MISC:

<http://blog.didierstevens.com/2010/06/29/quickpost-no-escape-from-pdf/>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

**CVE Reference:**

CVE-2010-1240 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **14580 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-1285) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified vectors, related to an "invalid pointer vulnerability," a different vulnerability than CVE-2010-2168 and CVE-2010-2201.

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

**References:**

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

\* VUPEN: VUPEN/ADV-2010-1636

<http://www.vupen.com/english/advisories/2010/1636>

\* SECTRACK: 1024159

<http://securitytracker.com/alerts/2010/Jun/1024159.html>

\* BID: 41232

<http://www.securityfocus.com/bid/41232>

**CVE Reference:**

CVE-2010-1285 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **14581 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-1295) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.

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

**References:**

\* VUPEN: VUPEN/ADV-2010-1636

<http://www.vupen.com/english/advisories/2010/1636>

\* SECTRACK: 1024159

<http://securitytracker.com/alerts/2010/Jun/1024159.html>

\* BID: 41230

<http://www.securityfocus.com/bid/41230>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

**CVE Reference:**

CVE-2010-1295 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **14582 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-1297) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted SWF content, related to authplay.dll and the ActionScript Virtual Machine 2 (AVM2) newfunction instruction, as exploited in the wild in June 2010.

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

**References:**

\* VUPEN: VUPEN/ADV-2010-1636

<http://www.vupen.com/english/advisories/2010/1636>

\* SECTRACK: 1024159

<http://securitytracker.com/alerts/2010/Jun/1024159.html>

\* BID: 41230

<http://www.securityfocus.com/bid/41230>  
\* NETVIGILANCE-UNKNOWN: 13787  
<http://www.exploit-db.com/exploits/13787>  
\* MISC:  
<http://blog.zynamics.com/2010/06/09/analyzing-the-currently-exploited-0-day-for-adobe-reader-and-adobe-flash/>  
\* MISC:  
<http://community.websense.com/blogs/securitylabs/archive/2010/06/09/having-fun-with-adobe-0-day-exploits.aspx>  
\* CONFIRM:  
<http://www.adobe.com/support/security/advisories/apsa10-01.html>  
\* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-14.html>  
\* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-15.html>  
\* REDHAT: RHSA-2010:0464  
<http://www.redhat.com/support/errata/RHSA-2010-0464.html>  
\* REDHAT: RHSA-2010:0470  
<http://www.redhat.com/support/errata/RHSA-2010-0470.html>  
\* SUSE: SUSE-SA:2010:024  
<http://lists.opensuse.org/opensuse-security-announce/2010-06/msg00000.html>  
\* SUSE: SUSE-SR:2010:013  
<http://lists.opensuse.org/opensuse-security-announce/2010-06/msg00001.html>  
\* TURBO: TLSA-2010-19  
<http://www.turbolinux.co.jp/security/2010/TLSA-2010-19j.txt>  
\* CERT: TA10-162A  
<http://www.us-cert.gov/cas/techalerts/TA10-162A.html>  
\* CERT: TA10-159A  
<http://www.us-cert.gov/cas/techalerts/TA10-159A.html>  
\* CERT-VN: VU#486225  
<http://www.kb.cert.org/vuls/id/486225>  
\* BID: 40586  
<http://www.securityfocus.com/bid/40586>  
\* BID: 40759  
<http://www.securityfocus.com/bid/40759>  
\* OSVDB: 65141  
<http://www.osvdb.org/65141>  
\* SECTRACK: 1024057  
<http://securitytracker.com/id?1024057>  
\* SECTRACK: 1024058  
<http://securitytracker.com/id?1024058>  
\* SECTRACK: 1024085  
<http://securitytracker.com/id?1024085>  
\* SECTRACK: 1024086  
<http://securitytracker.com/id?1024086>  
\* SECUNIA: 40026  
<http://secunia.com/advisories/40026>  
\* SECUNIA: 40034  
<http://secunia.com/advisories/40034>  
\* SECUNIA: 40144  
<http://secunia.com/advisories/40144>  
\* VUPEN: ADV-2010-1348  
<http://www.vupen.com/english/advisories/2010/1348>  
\* VUPEN: ADV-2010-1349  
<http://www.vupen.com/english/advisories/2010/1349>  
\* VUPEN: ADV-2010-1453  
<http://www.vupen.com/english/advisories/2010/1453>  
\* VUPEN: ADV-2010-1421  
<http://www.vupen.com/english/advisories/2010/1421>  
\* VUPEN: ADV-2010-1432  
<http://www.vupen.com/english/advisories/2010/1432>  
\* VUPEN: ADV-2010-1434  
<http://www.vupen.com/english/advisories/2010/1434>  
\* VUPEN: ADV-2010-1482  
<http://www.vupen.com/english/advisories/2010/1482>  
\* VUPEN: ADV-2010-1522  
<http://www.vupen.com/english/advisories/2010/1522>  
\* XF: adobe-authplay-code-execution(59137)  
<http://xforce.iss.net/xforce/xfdb/59137>

**CVE Reference:**

CVE-2010-1297 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14583 Adobe Acrobat / Reader arbitrary code execution Vulnerability (CVE-2010-2168) (Remote File Checking)**

Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified vectors, related to an "invalid pointer vulnerability," a different vulnerability than CVE-2010-1285 and CVE-2010-2201.

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

**References:**

- \* VUPEN: VUPEN/ADV-2010-1636  
<http://www.vupen.com/english/advisories/2010/1636>
- \* SECTRACK: 1024159  
<http://securitytracker.com/alerts/2010/Jun/1024159.html>
- \* BID: 41230  
<http://www.securityfocus.com/bid/41230>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

**CVE Reference:**

CVE-2010-2168 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

• **CVE-2010-2656 IBM CVSS 2.0 Score = 5.0**

The IBM BladeCenter with Advanced Management Module (AMM) firmware build ID BPET48L, and possibly other versions before 4.7 and 5.0, stores sensitive information under the web root with insufficient access control, which allows remote attackers to download (1) logs or (2) core files via direct requests, as demonstrated by a request for private/sdc.tgz.

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

**References:**

- BID: <http://www.securityfocus.com/bid/41383>
- EXPLOIT-DB: <http://www.exploit-db.com/exploits/14237/>
- MISC: <http://dsecrg.com/pages/vul/show.php?id=154>

**CVE Reference:** [CVE-2010-2656](http://cve.mitre.org)

• **CVE-2010-2654 IBM CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities on the IBM BladeCenter with Advanced Management Module (AMM) firmware build ID BPET48L, and possibly other versions before 4.7 and 5.0, allow remote attackers to inject arbitrary web script or HTML via the (1) INDEX or (2) IPADDR parameter to private/cindefn.php, (3) the domain parameter to private/power\_management\_policy\_options.php, the slot parameter to (4) private/pm\_temp.php or (5) private/power\_module.php, (6) the WEBINDEX parameter to private/blade\_leds.php, or (7) the SLOT parameter to private/ipmi\_bladestatus.php.

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

**References:**

- BID: <http://www.securityfocus.com/bid/41383>
- EXPLOIT-DB: <http://www.exploit-db.com/exploits/14237/>
- MISC: <http://dsecrg.com/pages/vul/show.php?id=154>

**CVE Reference:** [CVE-2010-2654](http://cve.mitre.org)

• **CVE-2010-2655 IBM CVSS 2.0 Score = 4.0**

Directory traversal vulnerability in private/file\_management.php on the IBM BladeCenter with Advanced Management Module (AMM) firmware build ID BPET48L, and possibly other versions before 4.7 and 5.0, allows remote authenticated users to list arbitrary directories and possibly have unspecified other impact via a .. (dot dot) in the DIR

parameter.

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

**References:**

BID: <http://www.securityfocus.com/bid/41383>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/14237/>

MISC: <http://dsecrg.com/pages/vul/show.php?id=154>

**CVE Reference:** [CVE-2010-2655](#)

• **CVE-2010-1574 Cisco CVSS 2.0 Score = 10.0**

IOS 12.2(52)SE and 12.2(52)SE1 on Cisco Industrial Ethernet (IE) 3000 series switches has (1) a community name of public for RO access and (2) a community name of private for RW access, which makes it easier for remote attackers to modify the configuration or obtain potentially sensitive information via SNMP requests, aka Bug ID CSCtf25589.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/60145>

BID: <http://www.securityfocus.com/bid/41436>

CISCO: [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080b3891f.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080b3891f.shtml)

SECTRAK: <http://securitytracker.com/id?1024173>

SECUNIA: <http://secunia.com/advisories/40407>

**CVE Reference:** [CVE-2010-1574](#)

• **CVE-2010-1575 Cisco CVSS 2.0 Score = 7.5**

The Cisco Content Services Switch (CSS) 11500 with software 08.20.1.01 conveys authentication data through ClientCert-\* headers but does not delete client-supplied ClientCert-\* headers, which might allow remote attackers to bypass authentication via crafted header data, as demonstrated by a ClientCert-Subject-CN header, aka Bug ID CSCsz04690.

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

**References:**

MISC: <http://www.vsecurity.com/resources/advisory/20100702-1/>

BID: <http://www.securityfocus.com/bid/41315>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/512144/100/0/threaded>

SECTRAK: <http://securitytracker.com/id?1024167>

**CVE Reference:** [CVE-2010-1575](#)

• **CVE-2010-1576 Cisco CVSS 2.0 Score = 7.5**

The Cisco Content Services Switch (CSS) 11500 with software before 8.20.4.02 and the Application Control Engine (ACE) 4710 with software before A2(3.0) do not properly handle use of LF, CR, and LFCR as alternatives to the standard CRLF sequence between HTTP headers, which allows remote attackers to bypass intended header insertions or conduct HTTP request smuggling attacks via crafted header data, as demonstrated by LF characters preceding ClientCert-Subject and ClientCert-Subject-CN headers, aka Bug ID CSCta04885.

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

**References:**

MISC: <http://www.vsecurity.com/resources/advisory/20100702-1/>

BID: <http://www.securityfocus.com/bid/41315>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/512144/100/0/threaded>

SECTRAK: <http://securitytracker.com/id?1024168>

SECTRAK: <http://securitytracker.com/id?1024167>

**CVE Reference:** [CVE-2010-1576](#)

• **CVE-2010-2629 Cisco CVSS 2.0 Score = 7.5**

The Cisco Content Services Switch (CSS) 11500 with software 8.20.4.02 and the Application Control Engine (ACE) 4710 with software A2(3.0) do not properly handle LF header terminators in situations where the GET line is terminated by CRLF, which allows remote attackers to conduct HTTP request smuggling attacks and possibly bypass intended header insertions via crafted header data, as demonstrated by an LF character between the ClientCert-Subject and ClientCert-Subject-CN headers. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-1576.

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

**References:**

MISC: <http://www.vsecurity.com/resources/advisory/20100702-1/>

BID: <http://www.securityfocus.com/bid/41315>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/512144/100/0/threaded>

SECTRAK: <http://securitytracker.com/id?1024168>

SECTRAK: <http://securitytracker.com/id?1024167>

**CVE Reference:** [CVE-2010-2629](#)

• **CVE-2010-2646 Google CVSS 2.0 Score = 9.3**

Google Chrome before 5.0.375.99 does not properly isolate sandboxed IFRAME elements, which has unspecified impact and remote attack vectors.

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

**References:**

CONFIRM: <http://googlechromereleases.blogspot.com/2010/07/stable-channel-update.html>

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=42980>

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=42575>

**CVE Reference:** [CVE-2010-2646](#)

**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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)