

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://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

Hackers share information. Two Energy Departments down after attack. Half of Rustock infected PCs cleaned. Data stolen the old-fashioned way.

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

- **Anonymous group creates whistleblower sites**

(Credit: LocalLeaks) (Credit: HackerLeaks)

A subgroup of the Anonymous hacker group has launched two WikiLeaks-type Web sites where insiders and other hackers can expose sensitive information from governments and corporations.

The LocalLeaks.tk site is for information related to corruption and wrongdoing at a local level, while the HackerLeaks.tk site is for any other stolen data. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20076261-245/anonymous-group-creates-whistleblower-sites/?part=rss&subj=ne

- **'Sophisticated' attack targets two Energy Dept. labs**

The Web sites of the Energy Department's Pacific Northwest National Lab and Jefferson National Lab were down today in the aftermath of "sophisticated" attacks, a spokesman at one of the labs told CNET.

The Richland, Wash.-based Pacific Northwest National Lab shut down its public Web site, Internet access, and e-mail service after the attack last Friday, spokesman Greg Koller said, adding that the Jefferson National Lab in Newport News, Va., was hit with a similar attack.

"No classified information has been compromised. About 20 percent we do here is classified," Koller said. "We have not found any indication that any of our unclassified information has been compromised [either]." Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20077268-245/sophisticated-attack-targets-two-energy-dept-labs/?part=rss&subj=

• After a botnet falls, infected PCs drop by more than half

More than half of Rustock-infected machines have been cleaned since Microsoft led a joint effort earlier this year to shut down the prolific botnet, according to new report released Tuesday by the software giant.

According to the "Battling the Rustock Threat" report, as of June 18, more than 700,000 IP addresses were infected with Rustock, down from more than 1.6 million on March 26.

"That's great news, and the infection reduction has happened much more quickly than it did for Waledac over a similar period of time last year, but we still have a long way to go," wrote Richard Boscovich, a Microsoft senior attorney, in a blog post. SC Magazine

Full Story :

http://www.scmagazineus.com/after-a-botnet-falls-infected-pcs-drop-by-more-than-half/article/206830/?utm_source=

• Report: Morgan Stanley warns 34,000 clients of data breach

Morgan Stanley Smith Barney has warned 34,000 customers that their addresses, account and tax ID numbers, and other data--including Social Security numbers for some--may have been stolen, the Credit.com news site reported today.

The data was reportedly on two CD-ROM discs that were password-protected but not encrypted, according to two letters Morgan Stanley sent to customers on June 24. The package containing the CDs was intact when it arrived at the New York State Department of Taxation and Finance but the CDs were missing when the package arrived on the desk of its intended recipient, Jim Wiggins, a Morgan Stanley Smith Barney spokesman told Credit.com. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20077001-245/report-morgan-stanley-warns-34000-clients-of-data-breach/?part=r

New Vulnerabilities Tested in SecureScout

• 19391 Adobe Acrobat / Reader 'SWF' File Remote Memory Corruption Vulnerability (CVE-2011-0611) (Remote File Checking)

A critical vulnerability exists in Flash Player 10.2.153.1 and earlier versions (Adobe Flash Player 10.2.154.25 and earlier for Chrome users) for Windows, Macintosh, Linux and Solaris, Adobe Flash Player 10.2.156.12 and earlier versions for Android, and the Authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.2) and earlier 10.x and 9.x versions for Windows and Macintosh operating systems.

This vulnerability (CVE-2011-0611) could cause a crash and potentially allow an attacker to take control of the affected system. There are reports that one of the vulnerabilities, CVE-2011-0611, is being actively exploited in the wild against both Adobe Flash Player, and Adobe Reader and Acrobat, as well as via a Flash (.swf) file embedded in a Microsoft Word (.doc) or Microsoft Excel (.xls) file delivered as an email attachment targeting the Windows platform. Adobe Reader X Protected Mode mitigations would prevent an exploit of this kind from executing.

Adobe recommends users of Adobe Reader X (10.0.2) for Macintosh update to Adobe Reader X (10.0.3). For users of Adobe Reader 9.4.3 for Windows and Macintosh, Adobe has made available the update, Adobe Reader 9.4.4. Adobe recommends users of Adobe Acrobat X (10.0.2) for Windows and Macintosh update to Adobe Acrobat X (10.0.3). Adobe recommends users of Adobe Acrobat 9.4.3 for Windows and Macintosh update to Adobe Acrobat 9.4.4. Because Adobe Reader X Protected Mode would prevent exploits of the type targeting CVE-2011-0611 from executing, Adobe is currently planning to address these issues in Adobe Reader X for Windows with the next quarterly security update for Adobe Reader, currently scheduled for June 14, 2011. For more information, see Security Bulletin AP5B11-08.

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

References:

* EXPLOIT-DB: 17175

<http://www.exploit-db.com/exploits/17175>

* MISC:

<http://bugix-security.blogspot.com/2011/04/cve-2011-0611-adobe-flash-zero-day.html>

* MISC:

<http://secunia.com/blog/210/>

* MISC:

<http://blogs.technet.com/b/mmpc/archive/2011/04/12/analysis-of-the-cve-2011-0611-adobe-flash-player-vulnerability-explo>

* MISC:

<http://contagiodump.blogspot.com/2011/04/apr-8-cve-2011-0611-flash-player-zero.html>

* CONFIRM:

<http://www.adobe.com/support/security/advisories/apsa11-02.html>

* CONFIRM:

<http://googlechromereleases.blogspot.com/2011/04/stable-channel-update.html>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-07.html>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-08.html>

* REDHAT: RHSA-2011:0451

<http://www.redhat.com/support/errata/RHSA-2011-0451.html>

* SUSE: SUSE-SA:2011:018

<http://lists.opensuse.org/opensuse-security-announce/2011-04/msg00004.html>

* CERT-VN: VU#230057

<http://www.kb.cert.org/vuls/id/230057>

* BID: 47314

<http://www.securityfocus.com/bid/47314>

* SECTRACK: 1025324

<http://www.securitytracker.com/id?1025324>

* SECTRACK: 1025325

<http://www.securitytracker.com/id?1025325>

* SECUNIA: 44141

<http://secunia.com/advisories/44141>

* SECUNIA: 44149

<http://secunia.com/advisories/44149>

* SECUNIA: 44119

<http://secunia.com/advisories/44119>

* VUPEN: ADV-2011-0922

<http://www.vupen.com/english/advisories/2011/0922>

* VUPEN: ADV-2011-0923

<http://www.vupen.com/english/advisories/2011/0923>

* VUPEN: ADV-2011-0924

<http://www.vupen.com/english/advisories/2011/0924>

* XF: adobe-flash-swf-doc-ce(66681)

<http://xforce.iss.net/xforce/xfdb/66681>

CVE Reference:

CVE-2011-0611 (cve.mitre.org, nvd.nist.gov)

● 19392 Adobe Acrobat / Reader CoolType library Remote Memory Corruption Vulnerability (Remote File Checking)

The CoolType library in Adobe Reader 9.x before 9.4.4 and 10.x through 10.0.1 on Windows, Adobe Reader 9.x before 9.4.4 and 10.x before 10.0.3 on Mac OS X, and Adobe Acrobat 9.x before 9.4.4 and 10.x before 10.0.3 on Windows and Mac OS X allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

Adobe recommends users of Adobe Reader X (10.0.2) for Macintosh update to Adobe Reader X (10.0.3). For users of Adobe Reader 9.4.3 for Windows and Macintosh, Adobe has made available the update, Adobe Reader 9.4.4. Adobe recommends users of Adobe Acrobat X (10.0.2) for Windows and Macintosh update to Adobe Acrobat X (10.0.3). Adobe recommends users of Adobe Acrobat 9.4.3 for Windows and Macintosh update to Adobe Acrobat 9.4.4. Because Adobe Reader X Protected Mode would prevent exploits of the type targeting CVE-2011-0611 from executing, Adobe is currently planning to address these issues in Adobe Reader X for Windows with the next quarterly security update for Adobe Reader, currently scheduled for June 14, 2011. Today's security updates are out-of-cycle updates.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-08.html>
* BID: 47531
<http://www.securityfocus.com/bid/47531>
* SECTRACK: 1025434
<http://securitytracker.com/id/1025434>

CVE Reference:

CVE-2011-0610 (cve.mitre.org, nvd.nist.gov)

• **19393 Adobe Acrobat / Reader buffer overflow Vulnerability (CVE-2011-2094) (Remote File Checking)**

Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2095 and CVE-2011-2097.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
* BID: 48240
<http://www.securityfocus.com/bid/48240>
* SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2094 (cve.mitre.org, nvd.nist.gov)

• **19394 Adobe Acrobat / Reader buffer overflow Vulnerability (CVE-2011-2095) (Remote File Checking)**

Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2094 and CVE-2011-2097.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
* BID: 48242
<http://www.securityfocus.com/bid/48242>
* SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2095 (cve.mitre.org, nvd.nist.gov)

• **19395 Adobe Acrobat / Reader heap overflow Vulnerability (CVE-2011-2096) (Remote File Checking)**

Heap-based buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
- * BID: 48243
<http://www.securityfocus.com/bid/48243>
- * SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2096 (cve.mitre.org, nvd.nist.gov)

• 19396 Adobe Acrobat / Reader buffer overflow Vulnerability (CVE-2011-2097) (Remote File Checking)

Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2094 and CVE-2011-2095.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
- * BID: 48244
<http://www.securityfocus.com/bid/48244>
- * SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2097 (cve.mitre.org, nvd.nist.gov)

• 19397 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2011-2098) (Remote File Checking)

Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 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-2011-2099.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
* BID: 48245
<http://www.securityfocus.com/bid/48245>
* SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2098 (cve.mitre.org, nvd.nist.gov)

• **19398 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2011-2099) (Remote File Checking)**

Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 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-2011-2098.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
* BID: 48246
<http://www.securityfocus.com/bid/48246>
* SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2099 (cve.mitre.org, nvd.nist.gov)

• **19399 Adobe Acrobat / Reader DLL loading Vulnerability (CVE-2011-2100) (Remote File Checking)**

Untrusted search path vulnerability in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
* BID: 48252
<http://www.securityfocus.com/bid/48252>
* SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2100 (cve.mitre.org, nvd.nist.gov)

• **19400 Adobe Acrobat / Reader cross document script execution Vulnerability (CVE-2011-2101) (Remote File Checking)**

Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X do not properly restrict script, which allows attackers to execute arbitrary code via a crafted document, related to a "cross document script execution vulnerability."

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

- * CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb11-16.html>
- * BID: 48255 <http://www.securityfocus.com/bid/48255>
- * SECTRACK: 1025658 <http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2101 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2011-2681 IBM CVSS 2.0 Score = 10.0**

IBM Rational DOORS Web Access 1.4.x before 1.4.0.4 does not properly handle exceptions, which has unspecified impact and remote attack vectors.

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

References:

- BID: <http://www.securityfocus.com/bid/48520>
- CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg27020404>
- AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM34972>
- SECUNIA: <http://secunia.com/advisories/45119>

CVE Reference: [CVE-2011-2681](http://cve.mitre.org/cve/2011/2681)

• **CVE-2011-2680 IBM CVSS 2.0 Score = 10.0**

Unspecified vulnerability in IBM Rational DOORS Web Access 1.4.x before 1.4.0.4 has unknown impact and remote attack vectors related to the "server error response."

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

References:

- BID: <http://www.securityfocus.com/bid/48520>
- CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg27020404>
- AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM34964>
- SECUNIA: <http://secunia.com/advisories/45119>

CVE Reference: [CVE-2011-2680](http://cve.mitre.org/cve/2011/2680)

• **CVE-2011-2679 IBM CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in IBM Rational DOORS Web Access 1.4.x before 1.4.0.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

BID: <http://www.securityfocus.com/bid/48520>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg27020404>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM34961>

SECUNIA: <http://secunia.com/advisories/45119>

CVE Reference: [CVE-2011-2679](#)

• **CVE-2011-2682 IBM CVSS 2.0 Score = 4.0**

The Login component in IBM Rational DOORS Web Access 1.4.x before 1.4.0.4 allows remote authenticated users to cause a denial of service (license consumption) by trying to login to DOORS Web Access with a new user account that has never been used for a DOORS login.

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

References:

BID: <http://www.securityfocus.com/bid/48520>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg27020404>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM38477>

CVE Reference: [CVE-2011-2682](#)

• **CVE-2011-2678 Cisco CVSS 2.0 Score = 6.8**

The Cisco VPN Client 5.0.7.0240 and 5.0.7.0290 on 64-bit Windows platforms uses weak permissions (NT AUTHORITY\INTERACTIVE:F) for cvpnd.exe, which allows local users to gain privileges by replacing this executable file with an arbitrary program, aka Bug ID CSCtn50645. NOTE: this vulnerability exists because of a CVE-2007-4415 regression.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/518638/100/0/threaded>

CISCO: <http://www.cisco.com/warp/public/707/cisco-sa-20070815-vpnclient.shtml>

MISC: <http://isc.sans.edu/diary.html?storyid=11125>

CVE Reference: [CVE-2011-2678](#)

• **CVE-2011-2597 Wireshark CVSS 2.0 Score = 4.3**

The Lucent/Ascend file parser in Wireshark 1.2.x before 1.2.18, 1.4.x through 1.4.7, and 1.6.0 allows remote attackers to cause a denial of service (infinite loop) via malformed packets.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/68335>

CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2011-11.html>

CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2011-10.html>

CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2011-09.html>

BID: <http://www.securityfocus.com/bid/48506>

SECTRACK: <http://securitytracker.com/id?1025738>

SECUNIA: <http://secunia.com/advisories/45086>

CVE Reference: [CVE-2011-2597](#)

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