

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 round of targeted attacks. Scammers use Japanese disaster. Medical ID theft on the rise. Phishers evading browser blacklists.

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

• New attacks leverage unpatched IE flaw, Microsoft warns

IDG News Service - An Internet Explorer flaw made public by a Google security researcher two months ago is now being used in online attacks.

The flaw, which has not yet been patched, has been used in "limited, targeted attacks," Microsoft said Friday in an update to its security advisory on the issue.

Google concurred, and offered a few more details. "We've noticed some highly targeted and apparently politically motivated attacks against our users," Google said in blog post. "We believe activists may have been a specific target. We've also seen attacks against users of another popular social site." Computerworld

Full Story :

http://www.computerworld.com/s/article/9214259/New_attacks_leverage_unpatched_IE_flaw_Microsoft_warns?source=...

• How to avoid disaster-related Internet scams

Scam e-mails are circulating that look like they come from the British Red Cross seeking donations for Japanese earthquake and tsunami survivors.

(Credit: AppRiver)

In every disaster scammers see an opportunity, and the crisis in Japan is no exception. Already there have been fake Red Cross e-mails circulating and there will no doubt be more scams coming. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20044320-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• **Medical ID theft on the rise, says new study**

Even though nearly 1.5 million Americans were victims of medical identity theft last year, many are doing little to protect their health records, according to a second annual study released Tuesday by The Ponemon Institute.

The report, which sampled nearly 1,700 consumers to determine how pervasive medical identity theft is in the United States and how it has affected American consumers, was sponsored by credit bureau Experian's ProtectMyID, an identity theft protection service.

Despite consumers' desire that their medical records remain private and frequent headlines of data breaches, a large number of respondents to the survey are not taking steps to ensure the safety of their health records, the survey found. SC Magazine

Full Story :

http://www.scmagazineus.com/medical-id-theft-on-the-rise-says-new-study/article/198370/?utm_source=feedburner&

• **Phishers use HTML attachments to evade browser blacklists**

Shown is an example of a phishing attack that encourages the recipient to download the HTML attachment and provide information. Note the poor grammar, "required informations," which should be a red flag.

(Credit: M86)

To get around phishing blacklists in browsers, scammers are luring people by using HTML attachments instead of URLs, a security firm is warning. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20043960-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• **19208 Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution (CVE-2006-3588) (MS06-069/923789) (Remote File Checking)**

Several remote code execution vulnerabilities exist in Macromedia Flash Player from Adobe because of the way that it handles Flash Animation (SWF) files. An attacker could exploit these vulnerabilities by constructing a specially crafted Flash Animation (SWF) file that could potentially allow remote code execution if a user visited a Web site containing the specially crafted SWF file. The specially crafted SWF file could also be sent as an e-mail attachment. A user would only be at risk if opening this e-mail attachment. An attacker who successfully exploited these vulnerabilities could take complete control of an affected system.

Flash Player versions 8.0.33.0, 7.0.68.0, or 7.0.66.0 fix the issue.

This test case checks for CVE-2006-3588.

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

References:

* MISC:

<http://www.fortinet.com/FortiGuardCenter/advisory/FG-2006-21.html>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb06-11.html>

* APPLE: APPLE-SA-2006-09-29

<http://lists.apple.com/archives/security-announce/2006/Sep/msg00002.html>

* GENTOO: GLSA-200610-02

<http://security.gentoo.org/glsa/glsa-200610-02.xml>

* MS: MS06-069

<http://www.microsoft.com/technet/security/bulletin/ms06-069.msp>

* REDHAT: RHSA-2006:0674
<http://www.redhat.com/support/errata/RHSA-2006-0674.html>

* SUSE: SUSE-SA:2006:053
http://www.novell.com/linux/security/advisories/2006_53_flashplayer.html

* CERT: TA06-318A
<http://www.us-cert.gov/cas/techalerts/TA06-318A.html>

* BID: 18894
<http://www.securityfocus.com/bid/18894>

* BID: 19980
<http://www.securityfocus.com/bid/19980>

* VUPEN: ADV-2006-2702
<http://www.vupen.com/english/advisories/2006/2702>

* VUPEN: ADV-2006-3577
<http://www.vupen.com/english/advisories/2006/3577>

* VUPEN: ADV-2006-3573
<http://www.vupen.com/english/advisories/2006/3573>

* VUPEN: ADV-2006-3852
<http://www.vupen.com/english/advisories/2006/3852>

* VUPEN: ADV-2006-4507
<http://www.vupen.com/english/advisories/2006/4507>

* OSVDB: 28733
<http://www.osvdb.org/28733>

* OVAL: oval:org.mitre.oval:def:432
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:432>

* SECTRACK: 1016449
<http://securitytracker.com/id?1016449>

* SECTRACK: 1016829
<http://securitytracker.com/id?1016829>

* SECUNIA: 21865
<http://secunia.com/advisories/21865>

* SECUNIA: 21901
<http://secunia.com/advisories/21901>

* SECUNIA: 22054
<http://secunia.com/advisories/22054>

* SECUNIA: 22187
<http://secunia.com/advisories/22187>

* SECUNIA: 22882
<http://secunia.com/advisories/22882>

* SECUNIA: 22268
<http://secunia.com/advisories/22268>

* XF: macromedia-swf-dos(27602)
<http://xforce.iss.net/xforce/xfdb/27602>

CVE Reference:

CVE-2006-3588 (cve.mitre.org, nvd.nist.gov)

• 19215 Adobe Flash Player 'SWF' File Remote Memory Corruption Vulnerability (Remote File Checking)

A critical vulnerability exists in Adobe Flash Player 10.2.152.33 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems (Adobe Flash Player 10.2.154.18 and earlier for Chrome users), Adobe Flash Player 10.1.106.16 and earlier versions for Android, and the authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.1) and earlier 10.x and 9.x versions for Windows and Macintosh operating systems.

This vulnerability (CVE-2011-0609) could cause a crash and potentially allow an attacker to take control of the affected system. There are reports that this vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Excel (.xls) file delivered as an email attachment. Adobe is not currently aware of attacks targeting Adobe Reader and Acrobat. Adobe Reader X Protected Mode mitigations would prevent an exploit of this kind from executing.

There are no current fixes for the issue.

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

References:

* BID: 46860
<http://www.securityfocus.com/bid/46860>

* CONFIRM:
<http://www.adobe.com/support/security/advisories/apsa11-01.html>

* CONFIRM:

<http://blogs.adobe.com/asset/2011/03/background-on-apsa11-01-patch-schedule.html>

CVE Reference:

CVE-2011-0609 (cve.mitre.org, nvd.nist.gov)

• 19216 Adobe Flash Player integer overflow vulnerability (CVE-2011-0558) (Remote File Checking)

Integer overflow in Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code via a large array length value in the ActionScript method of the Function class.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

* IDEFENSE: 20110208 Adobe Flash Player ActionScript Integer Overflow Vulnerability

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=893>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-02.html>

* REDHAT: RHSA-2011:0206

<http://www.redhat.com/support/errata/RHSA-2011-0206.html>

* REDHAT: RHSA-2011:0259

<http://www.redhat.com/support/errata/RHSA-2011-0259.html>

* SUSE: SUSE-SA:2011:009

<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>

* BID: 46194

<http://www.securityfocus.com/bid/46194>

* SECTRACK: 1025055

<http://www.securitytracker.com/id?1025055>

* SECUNIA: 43267

<http://secunia.com/advisories/43267>

* SECUNIA: 43292

<http://secunia.com/advisories/43292>

* SECUNIA: 43340

<http://secunia.com/advisories/43340>

* SECUNIA: 43351

<http://secunia.com/advisories/43351>

* VUPEN: ADV-2011-0348

<http://www.vupen.com/english/advisories/2011/0348>

* VUPEN: ADV-2011-0383

<http://www.vupen.com/english/advisories/2011/0383>

* VUPEN: ADV-2011-0402

<http://www.vupen.com/english/advisories/2011/0402>

* XF: flashplayer-actionscript-code-exec(65230)

<http://xforce.iss.net/xforce/xfdb/65230>

CVE Reference:

CVE-2011-0558 (cve.mitre.org, nvd.nist.gov)

• 19217 Adobe Flash Player memory corruption vulnerability (CVE-2011-0559) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted parameters to an unspecified ActionScript method that cause a parameter to be used as an object pointer, a different vulnerability than CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

* IDEFENSE: 20110208 Adobe Flash Player ActionScript Memory Corruption Vulnerability

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=894>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-02.html>

* REDHAT: RHSA-2011:0206

<http://www.redhat.com/support/errata/RHSA-2011-0206.html>

* REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
* SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
* SECTRACK: 1025055
<http://www.securitytracker.com/id?1025055>
* SECUNIA: 43267
<http://secunia.com/advisories/43267>
* SECUNIA: 43292
<http://secunia.com/advisories/43292>
* SECUNIA: 43340
<http://secunia.com/advisories/43340>
* SECUNIA: 43351
<http://secunia.com/advisories/43351>
* VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
* VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
* VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>

CVE Reference:

CVE-2011-0559 (cve.mitre.org, nvd.nist.gov)

• 19218 Adobe Flash Player memory corruption vulnerability (CVE-2011-0560) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-02.html>
* REDHAT: RHSA-2011:0206
<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
* REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
* SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
* CERT-VN: VU#812969
<http://www.kb.cert.org/vuls/id/812969>
* SECTRACK: 1025055
<http://www.securitytracker.com/id?1025055>
* SECUNIA: 43267
<http://secunia.com/advisories/43267>
* SECUNIA: 43292
<http://secunia.com/advisories/43292>
* SECUNIA: 43340
<http://secunia.com/advisories/43340>
* SECUNIA: 43351
<http://secunia.com/advisories/43351>
* VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
* VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
* VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>

CVE Reference:

CVE-2011-0560 (cve.mitre.org, nvd.nist.gov)

• 19219 Adobe Flash Player memory corruption vulnerability (CVE-2011-0561) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-02.html>
- * REDHAT: RHSA-2011:0206
<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
- * REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
- * SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
- * CERT-VN: VU#812969
<http://www.kb.cert.org/vuls/id/812969>
- * SECTrack: 1025055
<http://www.securitytracker.com/id?1025055>
- * SECUNIA: 43267
<http://secunia.com/advisories/43267>
- * SECUNIA: 43292
<http://secunia.com/advisories/43292>
- * SECUNIA: 43340
<http://secunia.com/advisories/43340>
- * SECUNIA: 43351
<http://secunia.com/advisories/43351>
- * VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
- * VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
- * VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>

CVE Reference:

CVE-2011-0561 (cve.mitre.org, nvd.nist.gov)

• 19220 Adobe Flash Player memory corruption vulnerability (CVE-2011-0571) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-02.html>
- * REDHAT: RHSA-2011:0206
<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
- * REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
- * SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
- * BID: 46190
<http://www.securityfocus.com/bid/46190>
- * OSVDB: 70915
<http://osvdb.org/70915>
- * SECTrack: 1025055
<http://www.securitytracker.com/id?1025055>
- * SECUNIA: 43267
<http://secunia.com/advisories/43267>

- * SECUNIA: 43292
<http://secunia.com/advisories/43292>
- * SECUNIA: 43340
<http://secunia.com/advisories/43340>
- * SECUNIA: 43351
<http://secunia.com/advisories/43351>
- * VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
- * VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
- * VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>
- * XF: adobe-flash-code-execution(65234)
<http://xforce.iss.net/xforce/xfdb/65234>

CVE Reference:

CVE-2011-0571 (cve.mitre.org, nvd.nist.gov)

• 19221 Adobe Flash Player memory corruption vulnerability (CVE-2011-0572) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-02.html>
- * REDHAT: RHSA-2011:0206
<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
- * REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
- * SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
- * BID: 46191
<http://www.securityfocus.com/bid/46191>
- * OSVDB: 70916
<http://osvdb.org/70916>
- * SECTRACK: 1025055
<http://www.securitytracker.com/id?1025055>
- * SECUNIA: 43267
<http://secunia.com/advisories/43267>
- * SECUNIA: 43292
<http://secunia.com/advisories/43292>
- * SECUNIA: 43340
<http://secunia.com/advisories/43340>
- * SECUNIA: 43351
<http://secunia.com/advisories/43351>
- * VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
- * VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
- * VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>
- * XF: adobe-player-code-exec(65235)
<http://xforce.iss.net/xforce/xfdb/65235>

CVE Reference:

CVE-2011-0572 (cve.mitre.org, nvd.nist.gov)

• 19222 Adobe Flash Player memory corruption vulnerability (CVE-2011-0573) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560,

CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-02.html>
- * REDHAT: RHSA-2011:0206
<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
- * REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
- * SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
- * BID: 46192
<http://www.securityfocus.com/bid/46192>
- * OSVDB: 70917
<http://osvdb.org/70917>
- * SECTrack: 1025055
<http://www.securitytracker.com/id?1025055>
- * SECUNIA: 43267
<http://secunia.com/advisories/43267>
- * SECUNIA: 43292
<http://secunia.com/advisories/43292>
- * SECUNIA: 43340
<http://secunia.com/advisories/43340>
- * SECUNIA: 43351
<http://secunia.com/advisories/43351>
- * VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
- * VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
- * VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>
- * XF: player-unspec-code-execution(65236)
<http://xforce.iss.net/xforce/xfdb/65236>

CVE Reference:

CVE-2011-0573 (cve.mitre.org, nvd.nist.gov)

• 19223 Adobe Flash Player memory corruption vulnerability (CVE-2011-0574) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-02.html>
- * REDHAT: RHSA-2011:0206
<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
- * REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
- * SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
- * BID: 46193
<http://www.securityfocus.com/bid/46193>
- * OSVDB: 70918
<http://osvdb.org/70918>
- * SECTrack: 1025055
<http://www.securitytracker.com/id?1025055>

* SECUNIA: 43267
<http://secunia.com/advisories/43267>
* SECUNIA: 43292
<http://secunia.com/advisories/43292>
* SECUNIA: 43340
<http://secunia.com/advisories/43340>
* SECUNIA: 43351
<http://secunia.com/advisories/43351>
* VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
* VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
* VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>
* XF: flash-player-code-exec(65237)
<http://xforce.iss.net/xforce/xfdb/65237>

CVE Reference:

CVE-2011-0574 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-1088 Apache CVSS 2.0 Score = 5.8

Apache Tomcat 7.x before 7.0.10 does not follow ServletSecurity annotations, which allows remote attackers to bypass intended access restrictions via HTTP requests to a web application.

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

References:

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1076586>

XF: <http://xforce.iss.net/xforce/xfdb/65971>

VUPEN: <http://www.vupen.com/english/advisories/2011/0563>

BID: <http://www.securityfocus.com/bid/46685>

OSVDB: <http://www.osvdb.org/71027>

CONFIRM: <http://tomcat.apache.org/security-7.html>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1077995>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1076587>

SECUNIA: <http://secunia.com/advisories/43684>

MLIST: <http://markmail.org/message/yzmyn44f5aetmm2r>

MLIST: <http://markmail.org/message/lzx5273wsgl5pob6>

MLIST:

http://mail-archives.apache.org/mod_mbox/www-announce/201103.mbox/%3C4D6E74FF.7050106@apache.org%3E

CVE Reference: [CVE-2011-1088](http://cve.mitre.org/cve/2011/1088)

• CVE-2011-1419 Apache CVSS 2.0 Score = 5.8

Apache Tomcat 7.x before 7.0.11, when web.xml has no security constraints, does not follow ServletSecurity annotations, which allows remote attackers to bypass intended access restrictions via HTTP requests to a web application. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-1088.

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

References:

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1079752>

XF: <http://xforce.iss.net/xforce/xfdb/65971>

VUPEN: <http://www.vupen.com/english/advisories/2011/0563>

BID: <http://www.securityfocus.com/bid/46685>

OSVDB: <http://www.osvdb.org/71027>

CONFIRM: <http://tomcat.apache.org/security-7.html>

SECUNIA: <http://secunia.com/advisories/43684>

MLIST: <http://markmail.org/message/yzmyn44f5aetmm2r>

MLIST: <http://markmail.org/message/lzx5273wsgl5pob6>

MLIST: <http://marc.info/?l=tomcat-user&m=129966773405409&w=2>

MLIST:

http://mail-archives.apache.org/mod_mbox/www-announce/201103.mbox/%3C4D6E74FF.7050106@apache.org%3E

CVE Reference: [CVE-2011-1419](#)

• **CVE-2011-0889 HP CVSS 2.0 Score = 9.3**

Unspecified vulnerability in HP Client Automation Enterprise (aka HPCA or Radia Notify) 5.11, 7.2, 7.5, 7.8, and 7.9 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2011/0651>

BID: <http://www.securityfocus.com/bid/46862>

SECTRAK: <http://securitytracker.com/id?1025205>

SECUNIA: <http://secunia.com/advisories/43766>

HP: <http://seclists.org/bugtraq/2011/Mar/132>

HP: <http://seclists.org/bugtraq/2011/Mar/132>

CVE Reference: [CVE-2011-0889](#)

• **CVE-2011-0280 HP CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in HP Power Manager (HPPM) 4.3.2 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the logType parameter to Contents/exportlogs.asp, (2) the Id parameter to Contents/pagehelp.asp, or the (3) SORTORD or (4) SORTCOL parameter to Contents/applicationlogs.asp. NOTE: some of these details are obtained from third party information.

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

References:

BID: <http://www.securityfocus.com/bid/46830>

SECUNIA: <http://secunia.com/advisories/43058>

HP: <http://archives.neohapsis.com/archives/bugtraq/2011-03/0111.html>

HP: <http://archives.neohapsis.com/archives/bugtraq/2011-03/0111.html>

CVE Reference: [CVE-2011-0280](#)

• **CVE-2011-1092 PHP CVSS 2.0 Score = 7.5**

Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.

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

References:

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/08/9>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/08/11>

CONFIRM:

http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/shmop/shmop.c?r1=306939&r2=309018&pathrev=309018

XF: <http://xforce.iss.net/xforce/xfdb/65988>

BID: <http://www.securityfocus.com/bid/46786>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/16966>

CVE Reference: [CVE-2011-1092](#)

• CVE-2011-1153 PHP CVSS 2.0 Score = 7.5

Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.

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

References:

CONFIRM: <http://svn.php.net/viewvc?view=revision&revision=309221>

MLIST: <http://openwall.com/lists/oss-security/2011/03/14/14>

XF: <http://xforce.iss.net/xforce/xfdb/66079>

BID: <http://www.securityfocus.com/bid/46854>

SECUNIA: <http://secunia.com/advisories/43744>

MLIST: <http://openwall.com/lists/oss-security/2011/03/14/24>

MLIST: <http://openwall.com/lists/oss-security/2011/03/14/13>

CONFIRM: <http://bugs.php.net/bug.php?id=54247>

CVE Reference: [CVE-2011-1153](#)

• CVE-2011-0609 Adobe CVSS 2.0 Score = 9.3

Unspecified vulnerability in Adobe Flash Player 10.2.154.13 and earlier on Windows, Mac OS X, Linux, and Solaris and 10.1.106.16 and earlier on Android, and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader and Acrobat 9.x through 9.4.2 and 10.x through 10.0.1 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content, as demonstrated by a .swf file embedded in an Excel spreadsheet, and as exploited in the wild in March 2011.

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

References:

BID: <http://www.securityfocus.com/bid/46860>

CONFIRM: <http://www.adobe.com/support/security/advisories/apsa11-01.html>

CONFIRM: <http://blogs.adobe.com/asset/2011/03/background-on-apsa11-01-patch-schedule.html>

CVE Reference: [CVE-2011-0609](#)

• CVE-2011-0695 Linux CVSS 2.0 Score = 5.7

Race condition in the cm_work_handler function in the InfiniBand driver (drivers/infiniband/core/cma.c) in Linux kernel 2.6.x allows remote attackers to cause a denial of service (panic) by sending an InfiniBand request while other request handlers are still running, which triggers an invalid pointer dereference.

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

References:

MLIST: <http://www.spinics.net/lists/linux-rdma/msg07448.html>

MLIST: <http://www.spinics.net/lists/linux-rdma/msg07447.html>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/11/1>

XF: <http://xforce.iss.net/xforce/xfdb/66056>

BID: <http://www.securityfocus.com/bid/46839>

SECUNIA: <http://secunia.com/advisories/43693>

CVE Reference: [CVE-2011-0695](#)

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