

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

Amazon users beware. class-action lawsuit over 'fire' bug. Supermarket terminals tampered with.

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

• Amazon users targeted with new phishing attack

Users who receive an email claiming their Amazon account is about to expire should think twice before clicking on any attachments.

That's because the message may have been sent from a cybercriminal, researchers at anti-virus firm Sophos have warned.

Attackers have been widely spamming messages - purportedly sent from Amazon - claiming users' accounts are about to be deactivated. The messages, of course, were not actually sent from Amazon and, in fact, aim to trick users into revealing their personal data. SC Magazine

Full Story :

http://www.scmagazineus.com/amazon-users-targeted-with-new-phishing-attack/article/218150/?utm_source=feedbu

• Group brings lawsuit against HP over printer "fire" bug

A New York man who owns two Hewlett-Packard printers has brought a class-action lawsuit against the technology giant over a vulnerability that opens the device up to a hacker attack.

The complaint, filed in U.S. District Court in San Jose, Calif., contends that HP knew of the vulnerability but failed to disclose its existence to customers, an unfair business practice.

"If [the] plaintiff and other members of the class had known about the defect in the software of the HP printers, they would not have purchased their HP printers," the suit alleges, adding its bringers suffered financial losses as a result. SC Magazine

Full Story :

http://www.scmagazineus.com/group-brings-lawsuit-against-hp-over-printer-fire-bug/article/218285/?utm_source=feed

• Vandals hack checkout terminals at California supermarkets

Criminals tampered with the credit and debit card readers placed on a number of self-checkout terminals belonging to a California supermarket chain, which resulted in dozens of instances of account fraud.

Twenty Lucky Supermarkets locations reported that their card readers were compromised, according to a Monday statement from parent Save Mart.

As of Monday, the company had received about 80 reports of employees or customers whose credit or debit card accounts were accessed to either conduct fraud or attempt to make a unauthorized transaction. SC Magazine

Full Story :

http://www.scmagazineus.com/vandals-hack-checkout-terminals-at-california-supermarkets/article/218511/?utm_source=feed

• Three "critical" patches to be in Microsoft security update

Microsoft is planning to next week release 14 patches to fix 20 vulnerabilities across its product line, the company announced Thursday.

Tuesday's monthly security update, to be released around 1 p.m. EST, will come with three "critical" and 11 "important" bulletins to plug holes in Windows, Office, Internet Explorer, Publisher and Windows Media Player. Most of the vulnerabilities, if exploited, can lead to remote code execution.

It is unclear if the update will include remediation for an unpatched Windows Kernel vulnerability, disclosed just prior to the November patches, which aids in the spread of the Duqu trojan. SC Magazine

Full Story :

http://www.scmagazineus.com/three-critical-patches-to-be-in-microsoft-security-update/article/218609/?utm_source=feed

New Vulnerabilities Tested in SecureScout

• 19667 Apache HTTP Server 'mod_proxy' Vulnerability via malformed URI

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions.

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

References:

* MISC:

<https://community.qualys.com/blogs/securitylabs/2011/11/23/apache-reverse-proxy-bypass-issue>

* CONFIRM:

<http://thread.gmane.org/gmane.comp.apache.devel/46440>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=756483

* URL: cve-2011-4317

<https://community.qualys.com/blogs/securitylabs/tags/cve-2011-4317>

CVE Reference:

CVE-2011-4317 (cve.mitre.org, nvd.nist.gov)

• 19668 PHP 'The _zip_name_locate function' denial of service Vulnerability via empty IP archive

The `_zip_name_locate` function in `zip_name_locate.c` in the Zip extension in PHP before 5.3.6 does not properly handle a `ZIPARCHIVE::FL_UNCHANGED` argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) `locateName` or (2) `statName` operation.

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

References:

- * SREASONRES: 20110318 libzip 0.9.3 `_zip_name_locate` NULL Pointer Dereference (incl PHP 5.3.5)
http://securityreason.com/achievement_securityalert/96
- * BUGTRAQ: 20110318 libzip 0.9.3 `_zip_name_locate` NULL Pointer Dereference (incl PHP 5.3.5)
<http://www.securityfocus.com/archive/1/archive/1/517065/100/0/threaded>
- * EXPLOIT-DB: 17004
<http://www.exploit-db.com/exploits/17004>
- * CONFIRM:
<http://bugs.php.net/bug.php?id=53885>
- * CONFIRM:
<http://svn.php.net/viewvc/?view=revision&revision=307867>
- * CONFIRM:
<http://www.php.net/ChangeLog-5.php>
- * CONFIRM:
<http://www.php.net/archive/2011.php>
- * CONFIRM:
http://www.php.net/releases/5_3_6.php
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=688735
- * CONFIRM:
<http://support.apple.com/kb/HT5002>
- * APPLE: APPLE-SA-2011-10-12-3
<http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>
- * DEBIAN: DSA-2266
<http://www.debian.org/security/2011/dsa-2266>
- * FEDORA: FEDORA-2011-3614
<http://lists.fedoraproject.org/pipermail/package-announce/2011-March/056642.html>
- * FEDORA: FEDORA-2011-3636
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/057709.html>
- * FEDORA: FEDORA-2011-3666
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/057710.html>
- * MANDRIVA: MDVSA-2011:052
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:052>
- * MANDRIVA: MDVSA-2011:053
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:053>
- * MANDRIVA: MDVSA-2011:099
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:099>
- * BID: 46354
<http://www.securityfocus.com/bid/46354>
- * SECUNIA: 43621
<http://secunia.com/advisories/43621>
- * SREASON: 8146
<http://securityreason.com/securityalert/8146>
- * VUPEN: ADV-2011-0744
<http://www.vupen.com/english/advisories/2011/0744>
- * VUPEN: ADV-2011-0764
<http://www.vupen.com/english/advisories/2011/0764>
- * VUPEN: ADV-2011-0890
<http://www.vupen.com/english/advisories/2011/0890>
- * XF: libzip-zipnamelocate-dos(66173)
<http://xforce.iss.net/xforce/xfdb/66173>

CVE Reference:

CVE-2011-0421 (cve.mitre.org, nvd.nist.gov)

• 19669 Mozilla Firefox bypassing intended access restrictions vulnerability via crafted web site

Mozilla Firefox before 3.6.23 and 4.x through 6 do not prevent the starting of a download in response to the holding of the Enter key, which allows user-assisted remote attackers to bypass intended access restrictions via a crafted web site.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-40.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=657462
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=662309
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=663899
- * DEBIAN: DSA-2312
<http://www.debian.org/security/2011/dsa-2312>
- * DEBIAN: DSA-2313
<http://www.debian.org/security/2011/dsa-2313>
- * DEBIAN: DSA-2317
<http://www.debian.org/security/2011/dsa-2317>
- * MANDRIVA: MDVSA-2011:139
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:139>
- * MANDRIVA: MDVSA-2011:140
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:140>
- * MANDRIVA: MDVSA-2011:141
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:141>
- * MANDRIVA: MDVSA-2011:142
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:142>
- * REDHAT: RHSA-2011:1341
<http://www.redhat.com/support/errata/RHSA-2011-1341.html>
- * SUSE: openSUSE-SU-2011:1076
<http://lists.opensuse.org/opensuse-updates/2011-10/msg00002.html>
- * SECUNIA: 46315
<http://secunia.com/advisories/46315>

CVE Reference:

CVE-2011-2372 (cve.mitre.org, nvd.nist.gov)

• 19670 Mozilla Firefox handling DOM objects vulnerability via unspecified vectors

The appendChild function in Mozilla Firefox before 3.6.20 and possibly other products does not properly handle DOM objects, which allows remote attackers to execute arbitrary code via unspecified vectors that lead to dereferencing of a "dangling pointer."

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-40.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=657462
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=662309
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=663899
- * DEBIAN: DSA-2312
<http://www.debian.org/security/2011/dsa-2312>
- * DEBIAN: DSA-2313
<http://www.debian.org/security/2011/dsa-2313>
- * DEBIAN: DSA-2317
<http://www.debian.org/security/2011/dsa-2317>
- * MANDRIVA: MDVSA-2011:139
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:139>
- * MANDRIVA: MDVSA-2011:140
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:140>
- * MANDRIVA: MDVSA-2011:141
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:141>
- * MANDRIVA: MDVSA-2011:142
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:142>
- * REDHAT: RHSA-2011:1341
<http://www.redhat.com/support/errata/RHSA-2011-1341.html>
- * SUSE: openSUSE-SU-2011:1076
<http://lists.opensuse.org/opensuse-updates/2011-10/msg00002.html>
- * SECUNIA: 46315

<http://secunia.com/advisories/46315>

CVE Reference:

CVE-2011-2378 (cve.mitre.org, nvd.nist.gov)

• 19671 Mozilla Firefox untrusted search path vulnerability in ThinkPadSensor::Startup function

Untrusted search path vulnerability in the ThinkPadSensor::Startup function in Mozilla Firefox before 3.6.20 allows local users to gain privileges by leveraging write access in an unspecified directory to place a Trojan horse DLL that is loaded into the running Firefox process.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-30.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=642469

* MANDRIVA: MDVSA-2011:127

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:127>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

* SUSE: SUSE-SU-2011:0967

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00027.html>

CVE Reference:

CVE-2011-2980 (cve.mitre.org, nvd.nist.gov)

• 19672 Mozilla Firefox event-management implementation vulnerability via crafted web site

The event-management implementation in Mozilla Firefox before 3.6.20 and possibly other products does not properly select the context for script to run in, which allows remote attackers to bypass the Same Origin Policy or execute arbitrary JavaScript code with chrome privileges via a crafted web site.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-30.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=614151

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=643450

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=650252

* DEBIAN: DSA-2295

<http://www.debian.org/security/2011/dsa-2295>

* DEBIAN: DSA-2296

<http://www.debian.org/security/2011/dsa-2296>

* DEBIAN: DSA-2297

<http://www.debian.org/security/2011/dsa-2297>

* MANDRIVA: MDVSA-2011:127

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:127>

* REDHAT: RHSA-2011:1164

<http://www.redhat.com/support/errata/RHSA-2011-1164.html>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

* SUSE: SUSE-SU-2011:0967

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00027.html>

CVE Reference:

CVE-2011-2981 (cve.mitre.org, nvd.nist.gov)

• 19673 Mozilla Firefox multiple unspecified vulnerability cause DOS via unknown vectors

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.20 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-30.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=541255
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=615970
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=632206
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=643062
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=674545
- * DEBIAN: DSA-2295
<http://www.debian.org/security/2011/dsa-2295>
- * DEBIAN: DSA-2296
<http://www.debian.org/security/2011/dsa-2296>
- * DEBIAN: DSA-2297
<http://www.debian.org/security/2011/dsa-2297>
- * MANDRIVA: MDVSA-2011:127
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:127>
- * REDHAT: RHSA-2011:1164
<http://www.redhat.com/support/errata/RHSA-2011-1164.html>
- * REDHAT: RHSA-2011:1165
<http://www.redhat.com/support/errata/RHSA-2011-1165.html>
- * REDHAT: RHSA-2011:1166
<http://www.redhat.com/support/errata/RHSA-2011-1166.html>
- * REDHAT: RHSA-2011:1167
<http://www.redhat.com/support/errata/RHSA-2011-1167.html>
- * SUSE: SUSE-SA:2011:037
<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>
- * SUSE: SUSE-SU-2011:0967
<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00027.html>
- * SECTRACK: 1025940
<http://www.securitytracker.com/id?1025940>

CVE Reference:

CVE-2011-2982 (cve.mitre.org, nvd.nist.gov)

• 19674 Mozilla Firefox handling RegExp.input vulnerability via crafted web site

Mozilla Firefox before 3.6.20 does not properly handle the RegExp.input property, which allows remote attackers to bypass the Same Origin Policy and read data from a different domain via a crafted web site, possibly related to a use-after-free.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-30.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=626297
- * DEBIAN: DSA-2295
<http://www.debian.org/security/2011/dsa-2295>
- * DEBIAN: DSA-2296
<http://www.debian.org/security/2011/dsa-2296>
- * DEBIAN: DSA-2297
<http://www.debian.org/security/2011/dsa-2297>
- * MANDRIVA: MDVSA-2011:127
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:127>
- * REDHAT: RHSA-2011:1164
<http://www.redhat.com/support/errata/RHSA-2011-1164.html>
- * REDHAT: RHSA-2011:1165
<http://www.redhat.com/support/errata/RHSA-2011-1165.html>
- * REDHAT: RHSA-2011:1167
<http://www.redhat.com/support/errata/RHSA-2011-1167.html>
- * SUSE: SUSE-SA:2011:037
<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>
- * SUSE: SUSE-SU-2011:0967

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00027.html>

* SECTRAK: 1025940

<http://www.securitytracker.com/id?1025940>

CVE Reference:

CVE-2011-2983 (cve.mitre.org, nvd.nist.gov)

• **19675 Mozilla Firefox handling tab element vulnerability with chrome privileges**

Mozilla Firefox before 3.6.20 does not properly handle the dropping of a tab element, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges by establishing a content area and registering for drop events.

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

References:

NULL

CVE Reference:

CVE-2011-2984 (cve.mitre.org, nvd.nist.gov)

• **19676 Mozilla Firefox multiple unspecified vulnerability causing DOS or arbitrary code via unknown vectors**

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 5 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=646825

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=648206

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=650273

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=650275

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=650732

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=651030

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=660517

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=662132

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=665518

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=667092

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=667315

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=667512

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=668245

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=669584

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-31.html>

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>

* SUSE: SUSE-SA:2011:037

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00023.html>

CVE Reference:

New Vulnerabilities found this Week

• CVE-2011-4695 Microsoft CVSS 2.0 Score = 6.9

Unspecified vulnerability in Microsoft Windows 7 SP1, when Java is installed, allows local users to bypass Internet Explorer sandbox restrictions and gain privileges via unknown vectors, as demonstrated by the White Phosphorus wp_ie_sandbox_escape module for Immunity CANVAS. NOTE: as of 20111207, this disclosure has no actionable information. However, because the module author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.

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

References:

MLIST: <https://lists.unityinc.com/pipermail/dailydave/2011-December/000402.html>

MISC: <http://partners.unityinc.com/movies/VulnDisco-Flash0day-v2.mov>

CVE Reference: [CVE-2011-4695](#)

• CVE-2010-5071 Microsoft CVSS 2.0 Score = 5.0

The JavaScript implementation in Microsoft Internet Explorer 8.0 and earlier does not properly restrict the set of values contained in the object returned by the getComputedStyle method, which allows remote attackers to obtain sensitive information about visited web pages by calling this method.

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

References:

MISC: <http://w2spconf.com/2010/papers/p26.pdf>

CVE Reference: [CVE-2010-5071](#)

• CVE-2011-4689 Microsoft CVSS 2.0 Score = 5.0

Microsoft Internet Explorer 6 through 9 does not prevent capture of data about the times of Same Origin Policy violations during IFRAME loading attempts, which makes it easier for remote attackers to determine whether a document exists in the browser cache via crafted JavaScript code.

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

References:

SECUNIA: <http://secunia.com/advisories/47129>

MISC: <http://lcamtuf.coredump.cx/cachetime/>

CVE Reference: [CVE-2011-4689](#)

• CVE-2002-2435 Microsoft CVSS 2.0 Score = 4.3

The Cascading Style Sheets (CSS) implementation in Microsoft Internet Explorer 8.0 and earlier does not properly handle the :visited pseudo-class, which allows remote attackers to obtain sensitive information about visited web pages via a crafted HTML document, a related issue to CVE-2010-2264.

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

References:

MISC: <http://w2spconf.com/2010/papers/p26.pdf>

MISC: http://bugzilla.mozilla.org/show_bug.cgi?id=147777

CVE Reference: [CVE-2002-2435](#)

• CVE-2011-4162 HP CVSS 2.0 Score = 7.5

The (1) AddUser, (2) AddUserEx, (3) RemoveUser, (4) RemoveUserByGuide, (5) RemoveUserEx, and (6) RemoveUserRegardless methods in HP Protect Tools Device Access Manager (PTDAM) before 6.1.0.1 allow remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a long SidString argument.

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

References:

MISC:

https://www.htbridge.ch/advisory/heap_memory_corruption_in_hp_device_access_manager_for_protect_tools_information

HP: <http://marc.info/?l=bugtraq&m=132284686204608&w=2>

HP: <http://marc.info/?l=bugtraq&m=132284686204608&w=2>

CVE Reference: [CVE-2011-4162](#)

• **CVE-2011-2653 Novell CVSS 2.0 Score = 10.0**

Directory traversal vulnerability in the rtrlet component in Novell ZENworks Asset Management (ZAM) 7.5 allows remote attackers to execute arbitrary code by uploading an executable file.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-342/>

CONFIRM: <http://download.novell.com/Download?buildid=hPvHtXeNmCU~>

CVE Reference: [CVE-2011-2653](#)

• **CVE-2011-2462 Adobe CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the U3D component in Adobe Reader and Acrobat 10.1.1 and earlier on Windows and Mac OS X, and Adobe Reader 9.x through 9.4.6 on UNIX, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, as exploited in the wild in December 2011.

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

References:

CONFIRM: <http://www.adobe.com/support/security/advisories/apsa11-04.html>

CVE Reference: [CVE-2011-2462](#)

• **CVE-2011-4694 Adobe CVSS 2.0 Score = 9.3**

Unspecified vulnerability in Adobe Flash Player 11.1.102.55 on Windows and Mac OS X allows remote attackers to execute arbitrary code via a crafted SWF file, as demonstrated by the second of two vulnerabilities exploited by the Intevydis vd_adobe_fp module in VulnDisco Step Ahead (SA). NOTE: as of 20111207, this disclosure has no actionable information. However, because the module author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.

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

References:

MLIST: <https://lists.immunityinc.com/pipermail/dailydave/2011-December/000402.html>

MISC: <http://partners.immunityinc.com/movies/VulnDisco-Flash0day-v2.mov>

CVE Reference: [CVE-2011-4694](#)

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@seurescout.net