

## 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

2010 rise in documented vulnerabilities. Attack toolkits becoming more sophisticated. Epsilon breach expected to result in attacks. U.S. may search computers without warrant.

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

### • Number of reported vulnerabilities spiked in 2010

Last year saw huge increases in the number of documented vulnerabilities and public exploit releases, according to the IBM X-Force 2010 Trend and Risk Report, released last week. A total of 8,562 vulnerabilities were documented in 2010, the greatest number of bugs ever disclosed during a single year. The number marked a 29 percent increase from 2009, according to the report.

The increase is partly a reflection of increased efforts to find and eliminate vulnerabilities through better software development and quality assurance process, Tom Cross, threat intelligence manager for IBM X-Force, told SCMagazineUS.com.

Companies often find vulnerabilities in their software while going through the process of improving their designs, he said. When this happens, the "responsible and accepted practice" is to issue a public advisory informing customers about the issue and how to obtain a fix. SC Magazine

Full Story :

### • **Attack toolkits to pose bigger problem for businesses**

Exploit toolkits are becoming increasingly sophisticated and effective, and they are poised to make their biggest impact yet this year, according to a report released Monday by HP Digital Vaccine Labs (DVLabs).

The report found that toolkits, or frameworks that are bought, sold or traded to simplify the launch of cyberattacks, had notably high success rates in the systems they infected.

Of the most popular toolkits, the Zombie Infection Kit, a tool for creating botnets, had the highest success rate with more than 15 percent of hosts infected, the report found. This means that if an attacker using the Zombie kit compromised a website that attracts 100,000 visitors a month, they would be able to exploit 15,000 host machines during that time. SC Magazine

Full Story :

[http://www.scmagazineus.com/attack-toolkits-to-pose-bigger-problem-for-businesses/article/199967/?utm\\_source=f](http://www.scmagazineus.com/attack-toolkits-to-pose-bigger-problem-for-businesses/article/199967/?utm_source=f)

### • **Experts warn of attacks as more Epsilon victims emerge**

Experts are warning users to be on high alert for targeted, spear phishing messages as companies continue to come forward that their email addresses were stolen as part of the massive Epsilon data breach disclosed five days ago.

The latest batch of affected organizations includes AbeBooks, Air Miles, Ameriprise Financial, Ameritrade, Beachbody, BeBe Stores, Eileen Fisher, Ethan Allen, Hilton HHonors program, Lacoste, McKinsey & Company, MoneyGram, Red Roof Inn, Robert Half, Target, Verizon and 1-800-Flowers, according to reports and breach notification letters.

Dallas-based email marketing service provider Epsilon on Friday revealed that hackers gained unauthorized entry to its email system to steal clients' customer data. The hijacked data includes email addresses and customer names. Customers may receive an increase in spam as a result of the breach, according to several notification letters. SC Magazine

Full Story :

[http://www.scmagazineus.com/experts-warn-of-attacks-as-more-epsilon-victims-emerge/article/200103/?utm\\_source](http://www.scmagazineus.com/experts-warn-of-attacks-as-more-epsilon-victims-emerge/article/200103/?utm_source)

### • **U.S. can conduct offsite searches of computers seized at borders, court rules**

Computerworld - Laptop computers and other digital devices carried into the U.S. may be seized from travelers without a warrant and sent to a secondary site for forensic inspection, the U.S. Court of Appeals for the Ninth Circuit ruled last week.

The ruling is the second in less than a year that allows the U.S. government to conduct warrantless, offsite searches of digital devices seized at the country's borders.

A federal court in Michigan last May issued a similar ruling in a case challenging the constitutionality of the warrantless seizure of a computer at the Detroit Metropolitan Airport. The defendant in a child pornography case also contended that a subsequent search of the device at a secondary computer forensic facility violated the Fourth Amendment of the Constitution. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9215554/U.S.\\_can\\_conduct\\_offsite\\_searches\\_of\\_computers\\_seized\\_at\\_bor](http://www.computerworld.com/s/article/9215554/U.S._can_conduct_offsite_searches_of_computers_seized_at_bor)

## **New Vulnerabilities Tested in SecureScout**

### • **19245 Adobe Flash Player memory corruption vulnerability (CVE-2010-3652) (Remote File Checking)**

Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, and CVE-2010-3650.

Adobe Flash Player versions 9.0.289.0, and 10.1.102.64 resolve the issue.

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

**References:**

\* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-26.html>  
\* CONFIRM:  
<http://support.apple.com/kb/HT4435>  
\* CONFIRM:  
[http://blogs.sun.com/security/entry/multiple\\_vulnerabilities\\_in\\_adobe\\_flash1](http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_adobe_flash1)  
\* APPLE: APPLE-SA-2010-11-10-1  
<http://lists.apple.com/archives/security-announce/2010/Nov/msg00000.html>  
\* GENTOO: GLSA-201101-09  
<http://security.gentoo.org/glsa/glsa-201101-09.xml>  
\* REDHAT: RHSA-2010:0829  
<http://www.redhat.com/support/errata/RHSA-2010-0829.html>  
\* REDHAT: RHSA-2010:0834  
<http://www.redhat.com/support/errata/RHSA-2010-0834.html>  
\* REDHAT: RHSA-2010:0867  
<http://www.redhat.com/support/errata/RHSA-2010-0867.html>  
\* SUSE: SUSE-SA:2010:055  
<http://lists.opensuse.org/opensuse-security-announce/2010-11/msg00002.html>  
\* BID: 44687  
<http://www.securityfocus.com/bid/44687>  
\* SECUNIA: 42183  
<http://secunia.com/advisories/42183>  
\* SECUNIA: 42926  
<http://secunia.com/advisories/42926>  
\* SECUNIA: 43026  
<http://secunia.com/advisories/43026>  
\* VUPEN: ADV-2010-2903  
<http://www.vupen.com/english/advisories/2010/2903>  
\* VUPEN: ADV-2010-2906  
<http://www.vupen.com/english/advisories/2010/2906>  
\* VUPEN: ADV-2010-2918  
<http://www.vupen.com/english/advisories/2010/2918>  
\* VUPEN: ADV-2011-0173  
<http://www.vupen.com/english/advisories/2011/0173>  
\* VUPEN: ADV-2011-0192  
<http://www.vupen.com/english/advisories/2011/0192>

#### CVE Reference:

CVE-2010-3652 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### ● 19246 Adobe Flash Player memory corruption vulnerability (CVE-2010-3654) (Remote File Checking)

Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris and 10.1.95.1 on Android, and authplay.dll (aka AuthPlayLib.bundle or libauthplay.so.0.0.0) in Adobe Reader and Acrobat 9.x through 9.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted SWF content, as exploited in the wild in October 2010.

Adobe Flash Player versions 9.0.289.0, and 10.1.102.64 resolve the issue.

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

#### References:

\* MISC:  
<http://contagiodump.blogspot.com/2010/10/potential-new-adobe-flash-player-zero.html>  
\* CONFIRM:  
<http://www.adobe.com/support/security/advisories/apsa10-05.html>  
\* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-26.html>  
\* CONFIRM:  
<http://support.apple.com/kb/HT4435>  
\* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-28.html>  
\* CONFIRM:  
[http://blogs.sun.com/security/entry/multiple\\_vulnerabilities\\_in\\_adobe\\_flash1](http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_adobe_flash1)  
\* APPLE: APPLE-SA-2010-11-10-1  
<http://lists.apple.com/archives/security-announce/2010/Nov/msg00000.html>  
\* GENTOO: GLSA-201101-08  
<http://security.gentoo.org/glsa/glsa-201101-08.xml>

\* GENTOO: GLSA-201101-09  
<http://security.gentoo.org/glsa/glsa-201101-09.xml>

\* REDHAT: RHSA-2010:0829  
<http://www.redhat.com/support/errata/RHSA-2010-0829.html>

\* REDHAT: RHSA-2010:0834  
<http://www.redhat.com/support/errata/RHSA-2010-0834.html>

\* REDHAT: RHSA-2010:0934  
<http://www.redhat.com/support/errata/RHSA-2010-0934.html>

\* REDHAT: RHSA-2010:0867  
<http://www.redhat.com/support/errata/RHSA-2010-0867.html>

\* SUSE: SUSE-SA:2010:058  
<http://lists.opensuse.org/opensuse-security-announce/2010-12/msg00001.html>

\* SUSE: SUSE-SA:2010:055  
<http://lists.opensuse.org/opensuse-security-announce/2010-11/msg00002.html>

\* TURBO: TLSA-2011-2  
<http://www.turbolinux.co.jp/security/2011/TLSA-2011-2j.txt>

\* CERT-VN: VU#298081  
<http://www.kb.cert.org/vuls/id/298081>

\* BID: 44504  
<http://www.securityfocus.com/bid/44504>

\* SECTRACK: 1024659  
<http://www.securitytracker.com/id?1024659>

\* SECTRACK: 1024660  
<http://www.securitytracker.com/id?1024660>

\* SECUNIA: 41917  
<http://secunia.com/advisories/41917>

\* SECUNIA: 42030  
<http://secunia.com/advisories/42030>

\* SECUNIA: 42183  
<http://secunia.com/advisories/42183>

\* SECUNIA: 42401  
<http://secunia.com/advisories/42401>

\* SECUNIA: 42926  
<http://secunia.com/advisories/42926>

\* SECUNIA: 43025  
<http://secunia.com/advisories/43025>

\* SECUNIA: 43026  
<http://secunia.com/advisories/43026>

\* VUPEN: ADV-2010-2903  
<http://www.vupen.com/english/advisories/2010/2903>

\* VUPEN: ADV-2010-2906  
<http://www.vupen.com/english/advisories/2010/2906>

\* VUPEN: ADV-2010-2918  
<http://www.vupen.com/english/advisories/2010/2918>

\* VUPEN: ADV-2010-3111  
<http://www.vupen.com/english/advisories/2010/3111>

\* VUPEN: ADV-2011-0173  
<http://www.vupen.com/english/advisories/2011/0173>

\* VUPEN: ADV-2011-0191  
<http://www.vupen.com/english/advisories/2011/0191>

\* VUPEN: ADV-2011-0192  
<http://www.vupen.com/english/advisories/2011/0192>

\* VUPEN: ADV-2011-0344  
<http://www.vupen.com/english/advisories/2011/0344>

#### CVE Reference:

CVE-2010-3654 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19247 Adobe Flash Player library-loading vulnerability (CVE-2010-3976) (Remote File Checking)

Untrusted search path vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse dwmapi.dll that is located in the same folder as a file that is processed by Flash Player.

Adobe Flash Player versions 9.0.289.0, and 10.1.102.64 resolve the issue.

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

#### References:

\* BUGTRAQ: 20100910 Adobe Flash Player IE version 10.1.x Insecure DLL Hijacking Vulnerability (dwmapi.dll)  
<http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2010-09/msg00070.html>

\* BUGTRAQ: 20101105 ASPR #2010-11-05-01: Remote Binary Planting in Adobe Flash Player  
<http://www.securityfocus.com/archive/1/archive/1/514653/100/0/threaded>

\* MISC:

[http://core.yehg.net/lab/pr0js/advisories/dll\\_hijacking/%5Bflash\\_player%5D\\_10.1.x\\_insecure\\_dll\\_hijacking\\_%28dwmapi.dll%29](http://core.yehg.net/lab/pr0js/advisories/dll_hijacking/%5Bflash_player%5D_10.1.x_insecure_dll_hijacking_%28dwmapi.dll%29)

\* MISC:

<http://www.acrossecurity.com/aspr/ASPR-2010-11-05-1-PUB.txt>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-26.html>

\* CONFIRM:

<http://support.apple.com/kb/HT4435>

\* APPLE: APPLE-SA-2010-11-10-1

<http://lists.apple.com/archives/security-announce/2010/Nov/msg00000.html>

\* GENTOO: GLSA-201101-09

<http://security.gentoo.org/glsa/glsa-201101-09.xml>

\* SUSE: SUSE-SA:2010:055

<http://lists.opensuse.org/opensuse-security-announce/2010-11/msg00002.html>

\* BID: 44671

<http://www.securityfocus.com/bid/44671>

\* SECUNIA: 43026

<http://secunia.com/advisories/43026>

\* VUPEN: ADV-2010-2903

<http://www.vupen.com/english/advisories/2010/2903>

\* VUPEN: ADV-2011-0192

<http://www.vupen.com/english/advisories/2011/0192>

#### CVE Reference:

CVE-2010-3976 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19248 Adobe Flash Player memory corruption vulnerability (CVE-2010-2884) (Remote File Checking)

Adobe Flash Player 10.1.82.76 and earlier on Windows, Mac OS X, Linux, and Solaris and 10.1.92.10 on Android; authplay.dll in Adobe Reader and Acrobat 9.x before 9.4; and authplay.dll in Adobe Reader and Acrobat 8.x before 8.2.5 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in September 2010.

Adobe Flash Player versions 10.1.85.3 resolve the issue.

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

#### References:

\* CONFIRM:

<http://www.adobe.com/support/security/advisories/apsa10-03.html>

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-22.html>

\* CONFIRM: apsb10-21

<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

\* CONFIRM:

<http://support.apple.com/kb/HT4435>

\* APPLE: APPLE-SA-2010-11-10-1

<http://lists.apple.com/archives/security-announce/2010/Nov/msg00000.html>

\* GENTOO: GLSA-201101-08

<http://security.gentoo.org/glsa/glsa-201101-08.xml>

\* GENTOO: GLSA-201101-09

<http://security.gentoo.org/glsa/glsa-201101-09.xml>

\* REDHAT: RHSA-2010:0706

<http://www.redhat.com/support/errata/RHSA-2010-0706.html>

\* REDHAT: RHSA-2010:0743

<http://www.redhat.com/support/errata/RHSA-2010-0743.html>

\* SUSE: SUSE-SA:2010:048

<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00001.html>

\* SUSE: SUSE-SR:2010:019

<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00006.html>

\* CERT: TA10-263A

<http://www.us-cert.gov/cas/techalerts/TA10-263A.html>

\* CERT: TA10-279A

<http://www.us-cert.gov/cas/techalerts/TA10-279A.html>

\* CERT-VN: VU#275289  
<http://www.kb.cert.org/vuls/id/275289>  
\* SECUNIA: 41434  
<http://secunia.com/advisories/41434>  
\* SECUNIA: 41435  
<http://secunia.com/advisories/41435>  
\* SECUNIA: 41443  
<http://secunia.com/advisories/41443>  
\* SECUNIA: 41526  
<http://secunia.com/advisories/41526>  
\* SECUNIA: 43025  
<http://secunia.com/advisories/43025>  
\* SECUNIA: 43026  
<http://secunia.com/advisories/43026>  
\* VUPEN: ADV-2010-2348  
<http://www.vupen.com/english/advisories/2010/2348>  
\* VUPEN: ADV-2010-2349  
<http://www.vupen.com/english/advisories/2010/2349>  
\* VUPEN: ADV-2011-0191  
<http://www.vupen.com/english/advisories/2011/0191>  
\* VUPEN: ADV-2011-0192  
<http://www.vupen.com/english/advisories/2011/0192>  
\* XF: adobe-flash-content-code-execution(61771)  
<http://xforce.iss.net/xforce/xfdb/61771>  
\* BID: 43205  
<http://www.securityfocus.com/bid/43205>

#### CVE Reference:

CVE-2010-2884 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19249 Adobe Flash Player memory corruption vulnerability (CVE-2010-0209) (Remote File Checking)

Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2213, CVE-2010-2214, and CVE-2010-2216.

Adobe Flash Player versions 9.0.280, and 10.1.82.76 resolve the issue.

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

#### References:

\* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-16.html>  
\* CONFIRM:  
<http://support.apple.com/kb/HT4435>  
\* APPLE: APPLE-SA-2010-11-10-1  
<http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html>  
\* GENTOO: GLSA-201101-09  
<http://security.gentoo.org/glsa/glsa-201101-09.xml>  
\* HP: HPSBMA02592  
<http://marc.info/?l=bugtraq&m=128767780602751&w=2>  
\* OVAL: oval:org.mitre.oval:def:11461  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11461>  
\* SECTRACK: 1024621  
<http://www.securitytracker.com/id?1024621>  
\* SECUNIA: 43026  
<http://secunia.com/advisories/43026>  
\* VUPEN: ADV-2011-0192  
<http://www.vupen.com/english/advisories/2011/0192>

#### CVE Reference:

CVE-2010-0209 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19250 Adobe Flash Player memory corruption vulnerability (CVE-2010-2188) (Remote File Checking)

Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code by calling the ActionScript native object 2200 connect method multiple times with different arguments, a different vulnerability than CVE-2010-2160,

CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, and CVE-2010-2187.

Adobe Flash Player versions 9.0.280, and 10.1.82.76 resolve the issue.

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

#### References:

- \* BUGTRAQ: 20100621 ZDI-10-111: Adobe Flash Player LocalConnection Memory Corruption Remote Code Execution Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/511924/100/0/threaded>
- \* MISC:  
<http://www.zerodayinitiative.com/advisories/ZDI-10-111>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-14.html>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-16.html>
- \* CONFIRM:  
<http://support.apple.com/kb/HT4435>
- \* APPLE: APPLE-SA-2010-11-10-1  
<http://lists.apple.com/archives/security-announce/2010/Nov/msg00000.html>
- \* GENTOO: GLSA-201101-09  
<http://security.gentoo.org/glsa/glsa-201101-09.xml>
- \* HP: HPSBMA02547  
[http://itrc.hp.com/service/cki/docDisplay.do?docId=emr\\_na-c02273751](http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02273751)
- \* 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>
- \* BID: 40759  
<http://www.securityfocus.com/bid/40759>
- \* BID: 40798  
<http://www.securityfocus.com/bid/40798>
- \* OVAL: oval:org.mitre.oval:def:6946  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6946>
- \* SECTRACK: 1024085  
<http://securitytracker.com/id?1024085>
- \* SECTRACK: 1024086  
<http://securitytracker.com/id?1024086>
- \* SECUNIA: 40144  
<http://secunia.com/advisories/40144>
- \* SECUNIA: 40545  
<http://secunia.com/advisories/40545>
- \* SECUNIA: 43026  
<http://secunia.com/advisories/43026>
- \* 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>
- \* VUPEN: ADV-2010-1793  
<http://www.vupen.com/english/advisories/2010/1793>
- \* VUPEN: ADV-2011-0192  
<http://www.vupen.com/english/advisories/2011/0192>

\* XF: adobe-fpair-memory-code-exec(59337)  
<http://xforce.iss.net/xforce/xfdb/59337>

#### CVE Reference:

CVE-2010-2188 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19251 Adobe Flash Player memory corruption vulnerability (CVE-2010-2213) (Remote File Checking)

Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-0209, CVE-2010-2214, and CVE-2010-2216.

Adobe Flash Player versions 9.0.280, and 10.1.82.76 resolve the issue.

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

#### References:

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-16.html>
- \* CONFIRM:  
<http://support.apple.com/kb/HT4435>
- \* APPLE: APPLE-SA-2010-11-10-1  
<http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html>
- \* GENTOO: GLSA-201101-09  
<http://security.gentoo.org/glsa/glsa-201101-09.xml>
- \* HP: HPSBMA02592  
<http://marc.info/?l=bugtraq&m=128767780602751&w=2>
- \* OVAL: oval:org.mitre.oval:def:10983  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10983>
- \* SECTRACK: 1024621  
<http://www.securitytracker.com/id?1024621>
- \* SECUNIA: 43026  
<http://secunia.com/advisories/43026>
- \* VUPEN: ADV-2011-0192  
<http://www.vupen.com/english/advisories/2011/0192>

#### CVE Reference:

CVE-2010-2213 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19252 Adobe Flash Player memory corruption vulnerability (CVE-2010-2214) (Remote File Checking)

Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-0209, CVE-2010-2213, and CVE-2010-2216.

Adobe Flash Player versions 9.0.280, and 10.1.82.76 resolve the issue.

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

#### References:

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb10-16.html>
- \* CONFIRM:  
<http://support.apple.com/kb/HT4435>
- \* APPLE: APPLE-SA-2010-11-10-1  
<http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html>
- \* GENTOO: GLSA-201101-09  
<http://security.gentoo.org/glsa/glsa-201101-09.xml>
- \* HP: HPSBMA02592  
<http://marc.info/?l=bugtraq&m=128767780602751&w=2>
- \* OVAL: oval:org.mitre.oval:def:11971  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11971>
- \* SECTRACK: 1024621  
<http://www.securitytracker.com/id?1024621>
- \* SECUNIA: 43026  
<http://secunia.com/advisories/43026>
- \* VUPEN: ADV-2011-0192

<http://www.vupen.com/english/advisories/2011/0192>

**CVE Reference:**

CVE-2010-2214 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19253 Adobe Flash Player click-jacking vulnerability (CVE-2010-2215) (Remote File Checking)**

Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to trick a user into (1) selecting a link or (2) completing a dialog, related to a "click-jacking" issue.

Adobe Flash Player versions 9.0.280, and 10.1.82.76 resolve the issue.

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

**References:**

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-16.html>

\* CONFIRM:

<http://support.apple.com/kb/HT4435>

\* APPLE: APPLE-SA-2010-11-10-1

<http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html>

\* GENTOO: GLSA-201101-09

<http://security.gentoo.org/glsa/glsa-201101-09.xml>

\* HP: HPSBMA02592

<http://marc.info/?l=bugtraq&m=128767780602751&w=2>

\* OVAL: oval:org.mitre.oval:def:11532

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11532>

\* SECTRACK: 1024621

<http://www.securitytracker.com/id?1024621>

\* SECUNIA: 43026

<http://secunia.com/advisories/43026>

\* VUPEN: ADV-2011-0192

<http://www.vupen.com/english/advisories/2011/0192>

**CVE Reference:**

CVE-2010-2215 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19254 Adobe Flash Player memory corruption vulnerability (CVE-2010-2216) (Remote File Checking)**

Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-0209, CVE-2010-2213, and CVE-2010-2214.

Adobe Flash Player versions 9.0.280, and 10.1.82.76 resolve the issue.

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

**References:**

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-16.html>

\* CONFIRM:

<http://support.apple.com/kb/HT4435>

\* APPLE: APPLE-SA-2010-11-10-1

<http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html>

\* GENTOO: GLSA-201101-09

<http://security.gentoo.org/glsa/glsa-201101-09.xml>

\* HP: HPSBMA02592

<http://marc.info/?l=bugtraq&m=128767780602751&w=2>

\* OVAL: oval:org.mitre.oval:def:11977

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11977>

\* SECTRACK: 1024621

<http://www.securitytracker.com/id?1024621>

\* SECUNIA: 43026

<http://secunia.com/advisories/43026>

\* VUPEN: ADV-2011-0192

<http://www.vupen.com/english/advisories/2011/0192>

**CVE Reference:**

## New Vulnerabilities found this Week

### • CVE-2011-1652 Microsoft CVSS 2.0 Score = 5.0

\*\* DISPUTED \*\* The default configuration of Microsoft Windows 7 immediately prefers a new IPv6 and DHCPv6 service over a currently used IPv4 and DHCPv4 service upon receipt of an IPv6 Router Advertisement (RA), and does not provide an option to ignore an unexpected RA, which allows remote attackers to conduct man-in-the-middle attacks on communication with external IPv4 servers via vectors involving RAs, a DHCPv6 server, and NAT-PT on the local network, aka a "SLAAC Attack." NOTE: it can be argued that preferring IPv6 complies with RFC 3484, and that attempting to determine the legitimacy of an RA is currently outside the scope of recommended behavior of host operating systems.

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

#### References:

MLIST: <https://lists.immunityinc.com/pipermail/dailydave/20110404/000122.html>

MISC: <http://resources.infosecinstitute.com/slaac-attack/>

CVE Reference: [CVE-2011-1652](#)

### • CVE-2011-0894 HP CVSS 2.0 Score = 5.5

Unspecified vulnerability in HP Operations 9.10 on UNIX platforms allows remote authenticated users to bypass intended access restrictions via unknown vectors.

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

#### References:

VUPEN: <http://www.vupen.com/english/advisories/2011/0837>

SECUNIA: <http://secunia.com/advisories/43985>

HP: <http://marc.info/?l=bugtraq&m=130166433409257&w=2>

HP: <http://marc.info/?l=bugtraq&m=130166433409257&w=2>

CVE Reference: [CVE-2011-0894](#)

### • CVE-2011-0891 HP CVSS 2.0 Score = 4.4

Unspecified vulnerability in the OS-Core.CORE2-KRN files in HP HP-UX B.11.23 and B.11.31 allows local users to cause a denial of service via unknown vectors.

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

#### References:

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02753287>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02753287>

CVE Reference: [CVE-2011-0891](#)

### • CVE-2011-0893 HP CVSS 2.0 Score = 4.3

Cross-site scripting (XSS) vulnerability in HP Operations 9.10 on UNIX platforms allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

#### References:

VUPEN: <http://www.vupen.com/english/advisories/2011/0837>

SECUNIA: <http://secunia.com/advisories/43985>

HP: <http://marc.info/?l=bugtraq&m=130166433409257&w=2>

HP: <http://marc.info/?l=bugtraq&m=130166433409257&w=2>

**CVE Reference:** [CVE-2011-0893](#)

• **CVE-2011-0895 HP CVSS 2.0 Score = 4.0**

Unspecified vulnerability in HP Network Node Manager i (NNMi) 9.0x allows remote authenticated users to obtain sensitive information via unknown vectors.

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

**References:**

HP: <http://marc.info/?l=bugtraq&m=130201751130787&w=2>

HP: <http://marc.info/?l=bugtraq&m=130201751130787&w=2>

**CVE Reference:** [CVE-2011-0895](#)

• **CVE-2011-1559 IBM CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the IBM Web Interface for Content Management (aka WEBi) 1.0.4 before FP3 has unknown impact and attack vectors.

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

**References:**

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg24029060>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11O13806>

SECUNIA: <http://secunia.com/advisories/43993>

**CVE Reference:** [CVE-2011-1559](#)

• **CVE-2011-1560 IBM CVSS 2.0 Score = 9.3**

solid.exe in IBM solidDB before 4.5.181, 6.0.x before 6.0.1067, 6.1.x and 6.3.x before 6.3.47, and 6.5.x before 6.5.0.3 uses a password-hash length specified by the client, which allows remote attackers to bypass authentication via a short length value.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/66455>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21474552>

**CVE Reference:** [CVE-2011-1560](#)

• **CVE-2011-1561 IBM CVSS 2.0 Score = 6.8**

The LDAP login feature in bos.rte.security 6.1.6.4 in IBM AIX 6.1, when ldap\_auth is enabled in ldap.cfg, allows remote attackers to bypass authentication via a login attempt with an arbitrary password.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2011/0836>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=isg11Z97416>

SECTRAK: <http://securitytracker.com/id?1025273>

SECUNIA: <http://secunia.com/advisories/43968>

CONFIRM: [http://aix.software.ibm.com/aix/efixes/security/ldapauth\\_advisory.asc](http://aix.software.ibm.com/aix/efixes/security/ldapauth_advisory.asc)

**CVE Reference:** [CVE-2011-1561](#)

## 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)