

## 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

From our developers:

This week, the team behind the SC Magazine Best Buy vulnerability scanner - yours truly, implemented a series of major enhancements to the framework used by the Authenticated Scan Remote File Check test method. One of the enhancements resulted in up to 33% memory reduction while at the same time starting the test cases faster. As part of another major enhancement our caching methodology has been expanded to include all calls to the remote registry leading to registry access dropping to a fraction giving us additional scanning speed and reduced stress of the remote target.

And from the news: Data breaches expensive. Industri want's incentives rather than laws. Music industri under attack in "war against copyright". More than 1 million web sites with malware.

Enjoy reading & Stay safe.

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

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

## Top Security News Stories this Week

- **Study finds \$214 per breached record in 2010**

Data breaches cost organizations \$7.2 million on average in 2010, up seven percent from \$6.8 million the previous year, according to the latest Cost of Data Breach study, released Tuesday by Symantec and the Ponemon Institute.

The sixth-annual study, which assessed the costs of activities resulting from the actual data breach experiences of 51 U.S.-based organizations, found that the incidents cost companies an average of \$214 per compromised record in

2010, up \$10 from the previous year. This is the fifth consecutive year that costs have increased.

The most expensive breach analyzed in the study cost \$35.3 million, while the lowest was \$780,000. The CEO of one company included in the data set was "extremely overwhelmed" by all of the costs associated with his organization's breach, Larry Ponemon, chairman and founder of the Ponemon Institute, told SCMagazineUS.com on Monday. SC Magazine

Full Story :

[http://www.scmagazineus.com/study-finds-214-per-breached-record-in-2010/article/197891/?utm\\_source=feedburner](http://www.scmagazineus.com/study-finds-214-per-breached-record-in-2010/article/197891/?utm_source=feedburner)

### • Industry groups push for security incentives, not laws

Instead of imposing additional security regulations, the U.S. government must work with the private sector to develop incentives that motivate companies to voluntarily adopt security best practices, a coalition of industry associations and civil liberties groups recommended in a white paper released Tuesday.

The paper, crafted by members of the Business Software Alliance (BSA), Center for Democracy & Technology, Internet Security Alliance (ISA), TechAmerica and the U.S. Chamber of Commerce, calls on the government to develop a "menu" of incentives, such as insurance discounts for enterprises and research-and-development tax credits for IT security vendors.

The paper builds on the conclusions of President Obama's nearly two-year old Cyberspace Policy Review by providing recommendations for ways the government and industry can work together to improve cybersecurity, Franck Journoud, director of cybersecurity policy at BSA, told SCMagazineUS.com on Wednesday. SC Magazine

Full Story :

[http://www.scmagazineus.com/industry-groups-push-for-security-incentives-not-laws/article/198010/?utm\\_source=feedburner](http://www.scmagazineus.com/industry-groups-push-for-security-incentives-not-laws/article/198010/?utm_source=feedburner)

### • BMI site latest target of Anonymous DDoS attacks

Anonymous announces its latest target: BMI.

(Credit: <http://anonnews.org/?p=press&a=item&i=687>)

The Web site of Broadcast Music Inc. (BMI) has been down since last night after being targeted by a distributed denial-of-service attack launched by the Anonymous hacker group as part of what it calls its "war on copyright." Cnet Security

Full Story :

[http://news.cnet.com/8301-27080\\_3-20041218-245.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-27080_3-20041218-245.html?part=rss&subj=news&tag=2547-1_3-0-20)

### • Report: Malware-laden sites double from a year ago

The number of infected Web sites tracked by Dasient has doubled in the past year to more than one million.

(Credit: Dasient)

More than 1 million Web sites were believed to be infected with malware in the fourth quarter of last year, nearly double from the previous year, according to figures released today by Dasient. Cnet Security

Full Story :

[http://news.cnet.com/8301-27080\\_3-20040367-245.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-27080_3-20040367-245.html?part=rss&subj=news&tag=2547-1_3-0-20)

## New Vulnerabilities Tested in SecureScout

### • 16363 Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution (CVE-2006-4640) (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-2006-4640.

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

## References:

- \* 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>
- \* MS: MS06-069  
<http://www.microsoft.com/technet/security/bulletin/ms06-069.msp>
- \* SUSE: SUSE-SA:2006:053  
[http://www.novell.com/linux/security/advisories/2006\\_53\\_flashplayer.html](http://www.novell.com/linux/security/advisories/2006_53_flashplayer.html)
- \* CERT: TA06-275A  
<http://www.us-cert.gov/cas/techalerts/TA06-275A.html>
- \* CERT: TA06-318A  
<http://www.us-cert.gov/cas/techalerts/TA06-318A.html>
- \* CERT-VN: VU#168372  
<http://www.kb.cert.org/vuls/id/168372>
- \* BID: 19980  
<http://www.securityfocus.com/bid/19980>
- \* OVAL: oval:org.mitre.oval:def:709  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:709>
- \* 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: 28734  
<http://www.osvdb.org/28734>
- \* SECUNIA: 21865  
<http://secunia.com/advisories/21865>
- \* SECUNIA: 22054  
<http://secunia.com/advisories/22054>
- \* SECUNIA: 22187  
<http://secunia.com/advisories/22187>
- \* SECUNIA: 22882  
<http://secunia.com/advisories/22882>
- \* XF: flashplayer-allowscriptaccess-security-bypass(28887)  
<http://xforce.iss.net/xforce/xfdb/28887>

## CVE Reference:

CVE-2006-4640 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19177 Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution (CVE-2006-3587) (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-2006-3587.

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

## References:

- \* MISC:  
<http://www.fortinet.com/FortiGuardCenter/advisory/FG-2006-20.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](http://www.novell.com/linux/security/advisories/2006_53_flashplayer.html)  
\* CERT: TA06-318A  
<http://www.us-cert.gov/cas/techalerts/TA06-318A.html>  
\* CERT-VN: VU#474593  
<http://www.kb.cert.org/vuls/id/474593>  
\* 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>  
\* OVAL: oval:org.mitre.oval:def:1050  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1050>  
\* OVAL: oval:org.mitre.oval:def:709  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:709>  
\* SECTRACK: 1016448  
<http://securitytracker.com/id?1016448>  
\* SECTRACK: 1016829  
<http://securitytracker.com/id?1016829>  
\* SECUNIA: 20971  
<http://secunia.com/advisories/20971>  
\* 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-file-code-execution(27601)  
<http://xforce.iss.net/xforce/xfdb/27601>

#### CVE Reference:

CVE-2006-3587 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19178 Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution (CVE-2006-3311) (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-2006-3311.

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

#### References:

\* BUGTRAQ: 20060912 Computer Terrorism (UK) :: Incident Response Centre - Adobe/Macromedia Flash Player Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/445825/100/0/threaded>

\* MISC:

<http://www.computerterrorism.com/research/ct12-09-2006.htm>

\* 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](http://www.novell.com/linux/security/advisories/2006_53_flashplayer.html)

\* CERT: TA06-275A

<http://www.us-cert.gov/cas/techalerts/TA06-275A.html>

\* CERT: TA06-318A

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

\* CERT-VN: VU#451380

<http://www.kb.cert.org/vuls/id/451380>

\* BID: 19980

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

\* 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>

\* OVAL: oval:org.mitre.oval:def:394

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:394>

\* 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>

\* SREASON: 1546

<http://securityreason.com/securityalert/1546>

\* XF: flashplayer-swf-string-bo(28886)

<http://xforce.iss.net/xforce/xfdb/28886>

#### CVE Reference:

CVE-2006-3311 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19207 Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution (CVE-2006-3014) (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-2006-3014.

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

#### References:

- \* FULLDISC: 20060620 Microsoft Excel File Embedded Shockwave Flash Object Exploit  
<http://archives.neohapsis.com/archives/fulldisclosure/2006-06/0414.html>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb06-11.html>
- \* MISC:  
<http://hackingspirits.com/vuln-rnd/vuln-rnd.html>
- \* MISC:  
<http://www.securiteam.com/windowsntfocus/5TP0M0KIUA.html>
- \* MS: MS06-069  
<http://www.microsoft.com/technet/security/bulletin/ms06-069.mspx>
- \* CERT: TA06-318A  
<http://www.us-cert.gov/cas/techalerts/TA06-318A.html>
- \* BID: 18583  
<http://www.securityfocus.com/bid/18583>
- \* BID: 19980  
<http://www.securityfocus.com/bid/19980>
- \* 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-2006-4507  
<http://www.vupen.com/english/advisories/2006/4507>
- \* OVAL: oval:org.mitre.oval:def:538  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:538>
- \* SECTRACK: 1016344  
<http://securitytracker.com/id?1016344>
- \* SECUNIA: 21865  
<http://secunia.com/advisories/21865>
- \* SECUNIA: 22882  
<http://secunia.com/advisories/22882>
- \* XF: excel-shockwave-code-execution(27312)  
<http://xfforce.iss.net/xfforce/xfdb/27312>

#### CVE Reference:

CVE-2006-3014 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19209 Adobe Flash Player DeclareFunction2 Actionscript tag buffer overflow (CVE-2007-6019) (Remote File Checking)

Adobe Flash Player 9.0.115.0 and earlier, and 8.0.39.0 and earlier, allows remote attackers to execute arbitrary code via an SWF file with a modified DeclareFunction2 Actionscript tag, which prevents an object from being instantiated properly.

Flash Player versions 9.0.124.0, and 8.0.42.0 fix the issue.

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

#### References:

- \* BUGTRAQ: 20080408 ZDI-08-021: Adobe Flash Player DeclareFunction2 Invalid Object Use Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/490623/100/0/threaded>
- \* BUGTRAQ: 20080414 Secunia Research: Adobe Flash Player "Declare Function (V7)" HeapOverflow  
<http://www.securityfocus.com/archive/1/archive/1/490824/100/0/threaded>
- \* MISC:  
<http://www.zerodayinitiative.com/advisories/ZDI-08-021>
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb08-11.html>
- \* APPLE: APPLE-SA-2008-05-28  
<http://lists.apple.com/archives/security-announce/2008/May/msg00001.html>
- \* GENTOO: GLSA-200804-21  
<http://www.gentoo.org/security/en/glsa/glsa-200804-21.xml>
- \* REDHAT: RHSA-2008:0221  
<http://www.redhat.com/support/errata/RHSA-2008-0221.html>
- \* SUNALERT: 238305  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-238305-1>
- \* SUSE: SUSE-SA:2008:022

<http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00006.html>

\* CERT: TA08-100A

<http://www.us-cert.gov/cas/techalerts/TA08-100A.html>

\* CERT: TA08-150A

<http://www.us-cert.gov/cas/techalerts/TA08-150A.html>

\* BID: 28694

<http://www.securityfocus.com/bid/28694>

\* OVAL: oval:org.mitre.oval:def:10160

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10160>

\* VUPEN: ADV-2008-1697

<http://www.vupen.com/english/advisories/2008/1697>

\* VUPEN: ADV-2008-1724

<http://www.vupen.com/english/advisories/2008/1724/references>

\* SECTRACK: 1019810

<http://www.securitytracker.com/id?1019810>

\* SECUNIA: 29763

<http://secunia.com/advisories/29763>

\* SECUNIA: 29865

<http://secunia.com/advisories/29865>

\* SECUNIA: 30430

<http://secunia.com/advisories/30430>

\* SECUNIA: 30507

<http://secunia.com/advisories/30507>

\* SREASON: 3805

<http://securityreason.com/securityalert/3805>

\* XF: adobe-flash-declarefunction2-bo(41717)

<http://xforce.iss.net/xforce/xfdb/41717>

#### CVE Reference:

CVE-2007-6019 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### ● 19210 Adobe Flash Player SWF files buffer overflow (CVE-2007-6242) (Remote File Checking)

Unspecified vulnerability in Adobe Flash Player 9.0.48.0 and earlier might allow remote attackers to execute arbitrary code via unknown vectors, related to "input validation errors."

Flash Player versions 9.0.115.0, 8.0.36.0, 7.0.71.0 fix the issue.

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

#### References:

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb07-20.html>

\* GENTOO: GLSA-200801-07

<http://www.gentoo.org/security/en/glsa/glsa-200801-07.xml>

\* REDHAT: RHSA-2007:1126

<http://www.redhat.com/support/errata/RHSA-2007-1126.html>

\* SUNALERT: 238305

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-238305-1>

\* SUSE: SUSE-SA:2007:069

<http://lists.opensuse.org/opensuse-security-announce/2007-12/msg00007.html>

\* CERT: TA07-355A

<http://www.us-cert.gov/cas/techalerts/TA07-355A.html>

\* BID: 26951

<http://www.securityfocus.com/bid/26951>

\* OVAL: oval:org.mitre.oval:def:9188

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9188>

\* VUPEN: ADV-2007-4258

<http://www.vupen.com/english/advisories/2007/4258>

\* VUPEN: ADV-2008-1724

<http://www.vupen.com/english/advisories/2008/1724/references>

\* SECTRACK: 1019116

<http://securitytracker.com/id?1019116>

\* SECUNIA: 28157

<http://secunia.com/advisories/28157>

\* SECUNIA: 28161

<http://secunia.com/advisories/28161>

\* SECUNIA: 28570

<http://secunia.com/advisories/28570>

- \* SECUNIA: 28213  
<http://secunia.com/advisories/28213>
- \* SECUNIA: 30507  
<http://secunia.com/advisories/30507>
- \* XF: adobe-swf-code-execution(39128)  
<http://xforce.iss.net/xforce/xfdb/39128>

**CVE Reference:**

CVE-2007-6242 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **19211 DirectShow Insecure Library Loading Vulnerability (MS11-015/2510030) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft DirectShow handles the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

**References:**

- \* MS: MS11-015  
<http://www.microsoft.com/technet/security/bulletin/ms11-015.msp>
- \* VUPEN: VUPEN/ADV-2011-0615  
<http://www.vupen.com/english/advisories/2011/0615>
- \* SECTRACK: 1025170  
<http://securitytracker.com/id/1025170>
- \* BID: 46682  
<http://www.securityfocus.com/bid/46682>

**CVE Reference:**

CVE-2011-0032 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **19212 DVR-MS Vulnerability (MS11-015/2510030) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Windows Media Player and Windows Media Center handle .dvr-ms files. This vulnerability could allow an attacker to execute arbitrary code if the attacker convinces a user to open a specially crafted .dvr-ms file. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

**References:**

- \* MS: MS11-015  
<http://www.microsoft.com/technet/security/bulletin/ms11-015.msp>
- \* VUPEN: VUPEN/ADV-2011-0615  
<http://www.vupen.com/english/advisories/2011/0615>
- \* SECTRACK: 1025170  
<http://securitytracker.com/id/1025170>
- \* BID: 46680  
<http://www.securityfocus.com/bid/46680>

**CVE Reference:**

CVE-2011-0042 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **19213 Remote Desktop Insecure Library Loading Vulnerability (MS11-017/2508062) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Windows Remote Desktop Client handles the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

**References:**

\* MS: MS11-017  
<http://www.microsoft.com/technet/security/bulletin/ms11-017.msp>  
\* VUPEN: VUPEN/ADV-2011-0616  
<http://www.vupen.com/english/advisories/2011/0616>  
\* SECTRACK: 1025172  
<http://www.securitytracker.com/id/1025172>  
\* BID: 46678  
<http://www.securityfocus.com/bid/46678>

**CVE Reference:**

CVE-2011-0029 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19214 Microsoft Groove Insecure Library Loading Vulnerability (MS11-016/2494047) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Groove 2007 handles the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

**References:**

\* MS: MS11-016  
<http://www.microsoft.com/technet/security/bulletin/ms11-016.msp>  
\* SECTRACK: 1025171  
<http://www.securitytracker.com/id/1025171>  
\* BID: 42695  
<http://www.securityfocus.com/bid/42695>  
\* EXPLOIT-DB: 14746  
<http://www.exploit-db.com/exploits/14746/>  
\* VUPEN: ADV-2010-2188  
<http://www.vupen.com/english/advisories/2010/2188>

**CVE Reference:**

CVE-2010-3146 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

• **CVE-2011-0029 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in the client in Microsoft Remote Desktop Connection 5.2, 6.0, 6.1, and 7.0 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .rdp file, aka "Remote Desktop Insecure Library Loading Vulnerability."Per: <http://cwe.mitre.org/data/definitions/426.html> 'CWE-426: Untrusted Search Path'

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-017.msp>

**CVE Reference:** [CVE-2011-0029](http://cve.mitre.org/cve/2011/0029)

• **CVE-2011-0032 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in DirectShow in Microsoft Windows Vista SP1 and SP2, Windows 7 Gold and SP1, Windows Server 2008 R2 and R2 SP1, and Windows Media Center TV Pack for Windows Vista allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a Digital Video Recording (.dvr-ms), Windows Recorded TV Show (.wtv), or .mpg file, aka "DirectShow Insecure Library Loading Vulnerability."Per: <http://cwe.mitre.org/data/definitions/426.html> 'CWE-426: Untrusted Search Path'

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-015.msp>

**CVE Reference:** [CVE-2011-0032](#)

• **CVE-2011-0042 Microsoft CVSS 2.0 Score = 9.3**

SBE.dll in the Stream Buffer Engine in Windows Media Player and Windows Media Center in Microsoft Windows XP SP2 and SP3, Windows XP Media Center Edition 2005 SP3, Windows Vista SP1 and SP2, Windows 7 Gold and SP1, and Windows Media Center TV Pack for Windows Vista does not properly parse Digital Video Recording (.dvr-ms) files, which allows remote attackers to execute arbitrary code via a crafted file, aka "DVR-MS Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-015.msp>

**CVE Reference:** [CVE-2011-0042](#)

• **CVE-2009-3028 Symantec CVSS 2.0 Score = 6.8**

The Altiris eXpress NS SC Download ActiveX control in AeXNSPkgDLLib.dll, as used in Symantec Altiris Deployment Solution 6.9.x, Notification Server 6.0.x, and Symantec Management Platform 7.0.x exposes an unsafe method, which allows remote attackers to force the download of arbitrary files and possibly execute arbitrary code via the DownloadAndInstall method.

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

**References:**

CONFIRM: <http://www.symantec.com/business/support/index?page=content&id=TECH44885>

CONFIRM:

[http://www.symantec.com/business/security\\_response/securityupdates/detail.jsp?fid=security\\_advisory&pvid=security\\_advisory](http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory)

BID: <http://www.securityfocus.com/bid/36346>

OSVDB: <http://www.osvdb.org/57893>

SECUNIA: <http://secunia.com/advisories/36679>

**CVE Reference:** [CVE-2009-3028](#)

• **CVE-2011-1309 IBM CVSS 2.0 Score = 7.5**

The Plug-in component in IBM WebSphere Application Server (WAS) before 7.0.0.15 does not properly handle trace requests, which has unspecified impact and attack vectors.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2011/0564>

BID: <http://www.securityfocus.com/bid/46736>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27014463>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM22860>

**CVE Reference:** [CVE-2011-1309](#)

• **CVE-2011-1343 IBM CVSS 2.0 Score = 7.5**

SQL injection vulnerability in the Web GUI in IBM Tivoli Netcool/OMNIBus before 7.3.0.4 allows remote attackers to execute arbitrary SQL commands via "dynamic SQL parameters."

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/65767>

VUPEN: <http://www.vupen.com/english/advisories/2011/0550>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg24029093>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1IZ83269>

SECUNIA: <http://secunia.com/advisories/43577>

**CVE Reference:** [CVE-2011-1343](#)

• **CVE-2011-1320 IBM CVSS 2.0 Score = 6.8**

The Security component in IBM WebSphere Application Server (WAS) 6.1.0.x before 6.1.0.35 and 7.x before 7.0.0.15, when the Tivoli Integrated Portal / embedded WebSphere Application Server (TIP/eWAS) framework is used, does not properly delete AuthCache entries upon a logout, which might allow remote attackers to access the server by leveraging an unattended workstation.

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

**References:**

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27014463>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM21536>

**CVE Reference:** [CVE-2011-1320](#)

• **CVE-2011-1321 IBM CVSS 2.0 Score = 6.5**

The AuthCache purge implementation in the Security component in IBM WebSphere Application Server (WAS) 6.1.0.x before 6.1.0.37 and 7.x before 7.0.0.15 does not purge a user from the PlatformCredential cache, which might allow remote authenticated users to gain privileges by leveraging a group membership specified in an old RACF Object (aka RACO).

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

**References:**

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27014463>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM24668>

**CVE Reference:** [CVE-2011-1321](#)

**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)