

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

Hacker defense via laser? Microsoft fixes bugs in silence. U.S. Treasury web infected. Consumer groups find online tracking levels alarming.

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

• Laser security coming to you?

Later this month at a conference in California, Dr. Jacob Scheuer of Tel Aviv University's School of Electrical Engineering will unveil a new strategy called the UFL (Ultra-Long Fiber Laser) to defend against hackers. Using fiber optic and computer technology, Scheuer's system uses binary lock-and-key data sent via light pulses that can be unlocked only by the receiver and sender.

The foundation of this system is a new laser invented by Scheuer that, he asserts, improves on current quantum key distribution schemes because it is simpler, faster, allows for longer communication links and is less expensive.

To explain how it works, he began by introducing an analogy: SC Magazine

Full Story :

http://www.scmagazineus.com/laser-security-coming-to-you/article/167976/?utm_source=feedburner&utm_medium=

• Two severe bugs silently fixed in recent Microsoft update

A recent Microsoft security patch silently fixed two severe vulnerabilities that were not disclosed, according to a security researcher at penetration testing vendor Core Security. Bulletin MS10-024, issued April 13 as part of Microsoft's regular Patch Tuesday update, silently fixed two flaws affecting Microsoft Exchange and Windows SMTP Services. The bugs could be leveraged to spoof responses to domain name system (DNS) queries and read a victim's email messages, according to researchers at Core Security.

The vulnerabilities, however, were not disclosed in Microsoft's security bulletin and were not given unique Common Vulnerabilities and Exposures (CVE) identifiers, yielding criticism that Microsoft downplayed the severity of the patch.

In its advisory, Microsoft described only denial-of-service and information-disclosure vulnerabilities. SC Magazine

Full Story :

http://www.scmagazineus.com/two-severe-bugs-silently-fixed-in-recent-microsoft-update/article/169585/?utm_source=

• U.S. Treasury websites infected with malicious script

Three U.S. Department of Treasury websites have been compromised to spread malware, a security researcher said Monday.

The sites belong to the U.S. Bureau of Engraving and Printing, whose primary mission is to produce paper currency for the federal government.

Roger Thompson, chief researcher officer of AVG, said the attackers injected a malicious IFRAME into the sites, causing visitors to unknowingly be redirected to a hacker-owned site in the Ukraine. The attack site, grepad.com, previously has been flagged as suspicious, according to a StopBadware report. SC Magazine

Full Story :

http://www.scmagazineus.com/us-treasury-websites-infected-with-malicious-script/article/169407/?utm_source=feed

• Consumer groups: Online tracking at 'alarming levels'

The tracking and targeting of consumers online has reached "alarming levels," warned a coalition of consumer and privacy groups in a letter to Congress on Monday.

The collection of 11 groups, which includes Consumer Action, Consumers Union, and the Electronic Frontier Foundation, said that because the online industry has been unable to regulate itself in protecting the privacy of consumers, it's time for government to step in.

"This tracking is an invasion of privacy...Consumers now rely on the Internet and other digital services for a wide variety of transactions," the groups wrote in their letter to Congress. "These include sensitive activities, such as health and financial matters. In these contexts, tracking people's every move online is not simply a matter of convenience or relevance. It presents serious risks to consumers' privacy, security and dignity." Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20004071-83.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 13755 Oracle Database Server - JavaVM component unspecified Vulnerability (apr-2010/CVE-2010-0867)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "JavaVM" component.

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

References:

* BID: 39427

<http://www.securityfocus.com/bid/39427>

* SECTrack: 1023858

<http://securitytracker.com/alerts/2010/Apr/1023858.html>

* VUPEN: VUPEN/ADV-2010-0878

<http://www.vupen.com/english/advisories/2010/0878>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>

* CERT: TA10-103B

<http://www.us-cert.gov/cas/techalerts/TA10-103B.html>

CVE Reference:

CVE-2010-0867 (cve.mitre.org, nvd.nist.gov)

• **13756 Oracle Database Server - XML DB component unspecified Vulnerability (apr-2010/CVE-2010-0851)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "XML DB" component.

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

References:

- * BID: 39434
<http://www.securityfocus.com/bid/39434>
- * SECTRAK: 1023858
<http://securitytracker.com/alerts/2010/Apr/1023858.html>
- * VUPEN: VUPEN/ADV-2010-0878
<http://www.vupen.com/english/advisories/2010/0878>
- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>
- * CERT: TA10-103B
<http://www.us-cert.gov/cas/techalerts/TA10-103B.html>
- * SECUNIA: 39438
<http://secunia.com/advisories/39438>

CVE Reference:

CVE-2010-0851 (cve.mitre.org, nvd.nist.gov)

• **13757 Oracle Database Server - Change Data Capture component unspecified Vulnerability (apr-2010/CVE-2010-0870)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Change Data Capture" component.

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

References:

- * BID: 39422
<http://www.securityfocus.com/bid/39422>
- * SECTRAK: 1023858
<http://securitytracker.com/alerts/2010/Apr/1023858.html>
- * VUPEN: VUPEN/ADV-2010-0878
<http://www.vupen.com/english/advisories/2010/0878>
- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>
- * CERT: TA10-103B
<http://www.us-cert.gov/cas/techalerts/TA10-103B.html>
- * SECUNIA: 39438
<http://secunia.com/advisories/39438>

CVE Reference:

CVE-2010-0870 (cve.mitre.org, nvd.nist.gov)

• **13758 Oracle Database Server - Audit component unspecified Vulnerability (apr-2010/CVE-2010-0854)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Audit" component.

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

References:

- * BID: 39428
<http://www.securityfocus.com/bid/39428>
- * SECTRAK: 1023858
<http://securitytracker.com/alerts/2010/Apr/1023858.html>
- * VUPEN: VUPEN/ADV-2010-0878
<http://www.vupen.com/english/advisories/2010/0878>
- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>
- * CERT: TA10-103B
<http://www.us-cert.gov/cas/techalerts/TA10-103B.html>
- * SECUNIA: 39438

<http://secunia.com/advisories/39438>

CVE Reference:

CVE-2010-0854 (cve.mitre.org, nvd.nist.gov)

• 18787 Mozilla Firefox - Remote code execution with use-after-free in nsTreeSelection Vulnerability (Remote File Checking)

Security researcher regenrecht reported via TippingPoint's Zero Day Initiative that a select event handler for XUL tree items could be called after the tree item was deleted. This results in the execution of previously freed memory which an attacker could use to crash a victim's browser and run arbitrary code on the victim's computer.

The issue has been fixed in Firefox 3.5.9 and 3.0.19.

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

References:

* BUGTRAQ: 20100402 ZDI-10-050: Mozilla Firefox nsTreeSelection EventListener Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/510542/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-050>

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-17.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=375928

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=540100

* DEBIAN: DSA-2027

<http://www.debian.org/security/2010/dsa-2027>

* FEDORA: FEDORA-2010-5526

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038367.html>

* FEDORA: FEDORA-2010-5539

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038378.html>

* FEDORA: FEDORA-2010-5561

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038406.html>

* MANDRIVA: MDVSA-2010:070

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>

* REDHAT: RHSA-2010:0332

<http://www.redhat.com/support/errata/RHSA-2010-0332.html>

* REDHAT: RHSA-2010:0333

<http://www.redhat.com/support/errata/RHSA-2010-0333.html>

* UBUNTU: USN-921-1

<http://ubuntu.com/usn/usn-921-1>

* SECTRAK: 1023780

<http://securitytracker.com/id?1023780>

* SECTRAK: 1023782

<http://securitytracker.com/id?1023782>

* SECUNIA: 38566

<http://secunia.com/advisories/38566>

* SECUNIA: 39117

<http://secunia.com/advisories/39117>

* SECUNIA: 39136

<http://secunia.com/advisories/39136>

* SECUNIA: 39204

<http://secunia.com/advisories/39204>

* SECUNIA: 39240

<http://secunia.com/advisories/39240>

* SECUNIA: 39242

<http://secunia.com/advisories/39242>

* SECUNIA: 39243

<http://secunia.com/advisories/39243>

* SECUNIA: 39308

<http://secunia.com/advisories/39308>

* SECUNIA: 39397

<http://secunia.com/advisories/39397>

* VUPEN: ADV-2010-0748

<http://www.vupen.com/english/advisories/2010/0748>

* VUPEN: ADV-2010-0764

<http://www.vupen.com/english/advisories/2010/0764>

* VUPEN: ADV-2010-0765

<http://www.vupen.com/english/advisories/2010/0765>

* VUPEN: ADV-2010-0781

<http://www.vupen.com/english/advisories/2010/0781>

* VUPEN: ADV-2010-0790

<http://www.vupen.com/english/advisories/2010/0790>

* VUPEN: ADV-2010-0849

<http://www.vupen.com/english/advisories/2010/0849>

* XF: firefox-nstreeselection-code-execution(57390)

<http://xforce.iss.net/xforce/xfdb/57390>

CVE Reference:

CVE-2010-0175 (cve.mitre.org, nvd.nist.gov)

• 18788 Mozilla Firefox - crashes in the browser engine Vulnerability (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances, and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Firefox 3.6.2, 3.5.9, 3.0.19.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-16.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=488850

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=491722

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=496011

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=499862

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=542136

* FEDORA: FEDORA-2010-5526

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038367.html>

* FEDORA: FEDORA-2010-5539

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038378.html>

* MANDRIVA: MDVSA-2010:070

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>

* UBUNTU: USN-921-1

<http://ubuntu.com/usn/usn-921-1>

* SECTRAK: 1023775

<http://securitytracker.com/id?1023775>

* SECTRAK: 1023781

<http://securitytracker.com/id?1023781>

* SECUNIA: 39136

<http://secunia.com/advisories/39136>

* SECUNIA: 39204

<http://secunia.com/advisories/39204>

* SECUNIA: 39242

<http://secunia.com/advisories/39242>

* SECUNIA: 39243

<http://secunia.com/advisories/39243>

* SECUNIA: 39397

<http://secunia.com/advisories/39397>

* VUPEN: ADV-2010-0748

<http://www.vupen.com/english/advisories/2010/0748>

* VUPEN: ADV-2010-0849

<http://www.vupen.com/english/advisories/2010/0849>

* XF: firefox-browser-eng-code-execution(57388)

<http://xforce.iss.net/xforce/xfdb/57388>

CVE Reference:

CVE-2010-0173 (cve.mitre.org, nvd.nist.gov)

• 18789 Mozilla Firefox - crashes in the browser engine, arbitrary code execution Vulnerability (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances, and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Firefox 3.6.2, 3.5.9.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-16.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=499844
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=546530
- * DEBIAN: DSA-2027
<http://www.debian.org/security/2010/dsa-2027>
- * FEDORA: FEDORA-2010-5526
<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038367.html>
- * FEDORA: FEDORA-2010-5539
<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038378.html>
- * FEDORA: FEDORA-2010-5561
<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038406.html>
- * MANDRIVA: MDVSA-2010:070
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>
- * REDHAT: RHSA-2010:0332
<http://www.redhat.com/support/errata/RHSA-2010-0332.html>
- * REDHAT: RHSA-2010:0333
<http://www.redhat.com/support/errata/RHSA-2010-0333.html>
- * UBUNTU: USN-921-1
<http://ubuntu.com/usn/usn-921-1>
- * SECTRACK: 1023775
<http://securitytracker.com/id?1023775>
- * SECTRACK: 1023781
<http://securitytracker.com/id?1023781>
- * SECUNIA: 38566
<http://secunia.com/advisories/38566>
- * SECUNIA: 39117
<http://secunia.com/advisories/39117>
- * SECUNIA: 39136
<http://secunia.com/advisories/39136>
- * SECUNIA: 39204
<http://secunia.com/advisories/39204>
- * SECUNIA: 39240
<http://secunia.com/advisories/39240>
- * SECUNIA: 39242
<http://secunia.com/advisories/39242>
- * SECUNIA: 39243
<http://secunia.com/advisories/39243>
- * SECUNIA: 39308
<http://secunia.com/advisories/39308>
- * SECUNIA: 39397
<http://secunia.com/advisories/39397>
- * VUPEN: ADV-2010-0748
<http://www.vupen.com/english/advisories/2010/0748>
- * VUPEN: ADV-2010-0764
<http://www.vupen.com/english/advisories/2010/0764>
- * VUPEN: ADV-2010-0765
<http://www.vupen.com/english/advisories/2010/0765>
- * VUPEN: ADV-2010-0781
<http://www.vupen.com/english/advisories/2010/0781>
- * VUPEN: ADV-2010-0790
<http://www.vupen.com/english/advisories/2010/0790>
- * VUPEN: ADV-2010-0849
<http://www.vupen.com/english/advisories/2010/0849>
- * XF: mozilla-browser-eng-code-exec(57389)

<http://xforce.iss.net/xforce/xfdb/57389>

CVE Reference:

CVE-2010-0174 (cve.mitre.org, nvd.nist.gov)

• 18790 Mozilla Firefox - Asynchronous Auth Prompt attaches to wrong window Vulnerability (Remote File Checking)

Mozilla developer Justin Dolske reported that the new asynchronous Authorization Prompt (HTTP username and password) was not always attached to the correct window. Although we have not demonstrated this, it may be possible for a malicious page to convince a user to open a new tab or popup to a trusted service and then have the HTTP authorization prompt from the malicious page appear to be the login prompt for the trusted page. This potential attack is greatly mitigated by the fact that very few web sites use HTTP authorization, preferring instead to use web forms and cookies.

The issue has been fixed in Firefox 3.6.2.
Only Firefox 3.6.x is affected.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-15.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=537862
- * MANDRIVA: MDVSA-2010:070
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>
- * BID: 38918
<http://www.securityfocus.com/bid/38918>
- * VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0172 (cve.mitre.org, nvd.nist.gov)

• 18791 Mozilla Firefox - Browser chrome defacement via cached XUL stylesheets Vulnerability (Remote File Checking)

Mozilla developer Wladimir Palant reported that stylesheets used in remote XUL documents can wind up in the XUL cache where it can later be accessed by browser chrome for use in styling the user interface. A malicious website could use this issue to pollute a user's XUL cache and change style attributes of their browser such as font size and color.

The issue has been fixed in Firefox 3.6.2, 3.5.8, and 3.0.18.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-14.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=535806
- * BID: 38918
<http://www.securityfocus.com/bid/38918>
- * VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0169 (cve.mitre.org, nvd.nist.gov)

• 18792 Mozilla Firefox - Content policy bypass with image preloading Vulnerability (Remote File Checking)

Mozilla developer Josh Soref of Nokia reported that documents failed to call certain security checks when attempting to preload images. Although the image content is not available to the page, it is possible to specify protocols that are normally not allowed in a web page such as file:. This includes internal schemes implemented by add-ons that might perform privileged actions resulting in something like a Cross-Site Request Forgery (CSRF) attack against the add-on. Potential severity would depend on the add-ons installed.

The issue has been fixed in Firefox 3.6.2.

This issue affects Firefox 3.6.x.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-13.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=540642
- * MANDRIVA: MDVSA-2010:070
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:070>
- * BID: 38918
<http://www.securityfocus.com/bid/38918>
- * VUPEN: ADV-2010-0692
<http://www.vupen.com/english/advisories/2010/0692>

CVE Reference:

CVE-2010-0168 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-1681 Microsoft CVSS 2.0 Score = 7.6

Buffer overflow in VISIODWG.DLL before 10.0.6880.4 in Microsoft Office Visio allows user-assisted remote attackers to execute arbitrary code via a crafted DXF file, a different vulnerability than CVE-2010-0254 and CVE-2010-0256.

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

References:

- BID: <http://www.securityfocus.com/bid/39836>
- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/511121/100/0/threaded>
- MISC: <http://www.coresecurity.com/content/ms-visio-dxf-buffer-overflow>

CVE Reference: [CVE-2010-1681](#)

• CVE-2010-1734 Microsoft CVSS 2.0 Score = 4.9

The SfnINSTRING function in win32k.sys in the kernel in Microsoft Windows 2000, XP, and Server 2003 allows local users to cause a denial of service (system crash) via a 0x18d value in the second argument (aka the Msg argument) of a PostMessage function call for the DDEMLEvent window.

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

References:

- BID: <http://www.securityfocus.com/bid/39631>
- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/510886/100/0/threaded>
- MISC: <http://vigilance.fr/vulnerability/Windows-denials-of-service-of-win32k-sys-9607>
- SECUNIA: <http://secunia.com/advisories/39456>

CVE Reference: [CVE-2010-1734](#)

• CVE-2010-1735 Microsoft CVSS 2.0 Score = 4.9

The SfnLOGONNOTIFY function in win32k.sys in the kernel in Microsoft Windows 2000, XP, and Server 2003 allows local users to cause a denial of service (system crash) via a 0x4c value in the second argument (aka the Msg argument) of a PostMessage function call for the DDEMLEvent window.

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

References:

- BID: <http://www.securityfocus.com/bid/39630>
- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/510884/100/0/threaded>

MISC: <http://vigilance.fr/vulnerability/Windows-denials-of-service-of-win32k-sys-9607>

SECUNIA: <http://secunia.com/advisories/39456>

CVE Reference: [CVE-2010-1735](#)

• **CVE-2010-1650 IBM CVSS 2.0 Score = 1.9**

IBM WebSphere Application Server (WAS) 6.0.x before 6.0.2.41, 6.1.x before 6.1.0.31, and 7.0.x before 7.0.0.11, when the -trace option (aka debugging mode) is enabled, executes debugging statements that print string representations of unspecified objects, which allows attackers to obtain sensitive information by reading the trace output.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM06839>

SECUNIA: <http://secunia.com/advisories/39628>

CVE Reference: [CVE-2010-1650](#)

• **CVE-2010-1651 IBM CVSS 2.0 Score = 1.9**

IBM WebSphere Application Server (WAS) 6.1.x before 6.1.0.31 and 7.0.x before 7.0.0.11, when Basic authentication and SIP tracing (aka full trace logging for SIP) are enabled, logs the entirety of all inbound and outbound SIP messages, which allows local users to obtain sensitive information by reading the trace log.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM08892>

SECUNIA: <http://secunia.com/advisories/39628>

CVE Reference: [CVE-2010-1651](#)

• **CVE-2010-0594 Cisco CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in Cisco Router and Security Device Manager (SDM) allows remote attackers to inject arbitrary web script or HTML via unknown vectors, aka Bug ID CSCtb38467.

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

References:

JVNDB: <http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-000014.html>

JVN: <http://jvn.jp/en/jp/JVN14313132/index.html>

CVE Reference: [CVE-2010-0594](#)

• **CVE-2010-1279 Adobe CVSS 2.0 Score = 9.3**

Multiple unspecified vulnerabilities in Adobe Photoshop CS4 11.x before 11.0.1 allow user-assisted remote attackers to execute arbitrary code via a crafted TIFF file.

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

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb10-10.html>

VUPEN: <http://www.vupen.com/english/advisories/2010/1049>

BID: <http://www.securityfocus.com/bid/39849>

SECUNIA: <http://secunia.com/advisories/39711>

CVE Reference: [CVE-2010-1279](#)

• **CVE-2010-1729 Apple CVSS 2.0 Score = 4.3**

WebKit.dll in WebKit, as used in Safari.exe 4.531.9.1 in Apple Safari, allows remote attackers to cause a denial of service (application crash) via JavaScript that writes <marquee> sequences in an infinite loop.

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

References:

MISC: <http://h.ackack.net/?p=258>

CVE Reference: [CVE-2010-1729](#)

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