

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

SSL certificate authority bankrupt after breach. Security leaders form new alliance. 3 men charged with hacking. Federal agencies required to report on security measures monthly.

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

• After breach, DigiNotar folds into voluntary bankruptcy

Embattled SSL certificate authority DigiNotar, responsible for issuing hundreds of counterfeit credentials after a hacker breached its infrastructure, apparently isn't too big to fail.

The Dutch-based company, owned by data security firm VASCO, was "declared bankrupt" on Tuesday by a District Court judge in The Netherlands.

DigiNotar's certificate services had been suspended since late August, when reports emerged that it had issued a phony SSL certificate for Google, which appeared in the wild, presumably so Iranian users could be spied on. SC Magazine

Full Story :

http://www.scmagazineus.com/after-breach-diginotar-folds-into-voluntary-bankruptcy/article/212424/?utm_source=f

• New cybersecurity alliance launches in Massachusetts

A collaboration among information security leaders in government, industry and academia has launched in Massachusetts with the goal of developing new data defense tactics.

Dubbed the Advanced Cyber Security Center (ACSC), the operation will be based at the Bedford, Mass. campus of MITRE, a nonprofit that explores new technologies for government and private industry clients. The initiative will also operate out of five colleges in the state - MIT, Harvard, Boston University, Northeastern and the University of Massachusetts.

The facility will draw on guidance from expert practitioners in health care, energy, defense, financial services and technology to share best practices, conduct real-time threat analysis and develop next-generation secure computing architecture. SC Magazine

Full Story :

http://www.scmagazineus.com/new-cybersecurity-alliance-launches-in-massachusetts/article/212582/?utm_source=

• **Seattle men indicted on hacking, fraud charges**

Three Seattle men were charged this week with hacking into the networks of more than a dozen businesses to steal online banking credentials and other data used to commit a variety of fraudulent acts. Joshua Witt, 34, and Brad Lowe and John Griffin, both 36, were charged in a 10-count federal indictment that accuses them of conspiracy, damaging computers, access device fraud and aggravated identity theft, according to a news release Wednesday from the U.S. Attorney's Office in Seattle.

Led by Griffin, the trio carried out the fraud from 2008 until 2010, according to prosecutors. During this time, they broke into more than a dozen business networks, and stole credit card numbers that were used to purchase tens of thousands of dollars in equipment and luxury goods. SC Magazine

Full Story :

http://www.scmagazineus.com/seattle-men-indicted-on-hacking-fraud-charges/article/212645/?utm_source=feedburn

• **FISMA compliance to require monthly reports**

Federal agencies soon will be required to report on their information security health on a monthly basis, instead of annually, according to a memo from the federal Office of Management and Budget.

As part of their compliance with the Federal Information Security Management Act (FISMA), agencies must, beginning next month, submit data from their automated security management tools into CyberScope, an application that went online in 2009, and is used to securely and efficiently report security-related information and provide analysis.

"This shift from the once-a-year FISMA reporting process to a monthly reporting of key metrics through CyberScope allows security practitioners to make decisions using more information - delivered more quickly than ever before," OMB Director Jacob Lew wrote in the memo, issued last week. SC Magazine

Full Story :

http://www.scmagazineus.com/fisma-compliance-to-require-monthly-reports/article/212348/?utm_source=feedburn

New Vulnerabilities Tested in SecureScout

• **19471 Mozilla Firefox - Non-whitelisted site can trigger xpinstall (Remote File Checking)**

Mozilla Firefox before 5.0 does not properly enforce the whitelist for the xpinstall functionality, which allows remote attackers to trigger an installation dialog for a (1) add-on or (2) theme via unspecified vectors.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-28.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=645699

* SUSE: SUSE-SA:2011:028

<http://lists.opensuse.org/opensuse-security-announce/2011-07/msg00001.html>

CVE Reference:

CVE-2011-2370 (cve.mitre.org, nvd.nist.gov)

• **19472 Mozilla Firefox - Miscellaneous memory safety hazards (CVE-2011-2374) (Remote File Checking)**

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.18 and 4.x through 4.0.1, and Thunderbird before 3.1.11, 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: **DoS / Attack** Risk: **High**

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-19.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=626262
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=629858
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=639648
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=642338
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=642734
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=643051
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=645572
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=646662
- * DEBIAN: DSA-2268
<http://www.debian.org/security/2011/dsa-2268>
- * DEBIAN: DSA-2269
<http://www.debian.org/security/2011/dsa-2269>
- * DEBIAN: DSA-2273
<http://www.debian.org/security/2011/dsa-2273>
- * MANDRIVA: MDVSA-2011:111
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:111>
- * REDHAT: RHSA-2011:0885
<http://www.redhat.com/support/errata/RHSA-2011-0885.html>
- * REDHAT: RHSA-2011:0886
<http://www.redhat.com/support/errata/RHSA-2011-0886.html>
- * REDHAT: RHSA-2011:0887
<http://www.redhat.com/support/errata/RHSA-2011-0887.html>
- * REDHAT: RHSA-2011:0888
<http://www.redhat.com/support/errata/RHSA-2011-0888.html>
- * SUSE: SUSE-SA:2011:028
<http://lists.opensuse.org/opensuse-security-announce/2011-07/msg00001.html>

CVE Reference:

CVE-2011-2374 (cve.mitre.org, nvd.nist.gov)

• 19473 Mozilla Firefox - Miscellaneous memory safety hazards (CVE-2011-2375) (Remote File Checking)

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 5.0 and Thunderbird through 3.1.11 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

This issue affects Firefox version 4.X specifically.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-19.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=597162
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=643839
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=643927
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=648022

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=648705
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=652401
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=653026
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=653238
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=654015
* MANDRIVA: MDVSA-2011:111
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:111>
* REDHAT: RHSA-2011:0885
<http://www.redhat.com/support/errata/RHSA-2011-0885.html>
* REDHAT: RHSA-2011:0886
<http://www.redhat.com/support/errata/RHSA-2011-0886.html>
* REDHAT: RHSA-2011:0887
<http://www.redhat.com/support/errata/RHSA-2011-0887.html>
* REDHAT: RHSA-2011:0888
<http://www.redhat.com/support/errata/RHSA-2011-0888.html>

CVE Reference:

CVE-2011-2375 (cve.mitre.org, nvd.nist.gov)

● 19474 Mozilla Firefox - Miscellaneous memory safety hazards (CVE-2011-2376) (Remote File Checking)

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.18 and Thunderbird before 3.1.11 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: **DoS / Attack** Risk: **High**

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-19.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=635235
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=650874
* DEBIAN: DSA-2268
<http://www.debian.org/security/2011/dsa-2268>
* DEBIAN: DSA-2269
<http://www.debian.org/security/2011/dsa-2269>
* DEBIAN: DSA-2273
<http://www.debian.org/security/2011/dsa-2273>
* MANDRIVA: MDVSA-2011:111
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:111>
* REDHAT: RHSA-2011:0885
<http://www.redhat.com/support/errata/RHSA-2011-0885.html>
* REDHAT: RHSA-2011:0886
<http://www.redhat.com/support/errata/RHSA-2011-0886.html>
* REDHAT: RHSA-2011:0887
<http://www.redhat.com/support/errata/RHSA-2011-0887.html>
* REDHAT: RHSA-2011:0888
<http://www.redhat.com/support/errata/RHSA-2011-0888.html>
* SUSE: SUSE-SA:2011:028
<http://lists.opensuse.org/opensuse-security-announce/2011-07/msg00001.html>

CVE Reference:

CVE-2011-2376 (cve.mitre.org, nvd.nist.gov)

● 19475 Mozilla Firefox - Miscellaneous memory safety hazards (CVE-2011-2364) (Remote File Checking)

Unspecified vulnerability in the browser engine in Mozilla Firefox 3.6.x before 3.6.18 and Thunderbird before 3.1.11 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-2365.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-19.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=651990
- * MANDRIVA: MDVSA-2011:111
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:111>
- * REDHAT: RHSA-2011:0885
<http://www.redhat.com/support/errata/RHSA-2011-0885.html>
- * REDHAT: RHSA-2011:0886
<http://www.redhat.com/support/errata/RHSA-2011-0886.html>
- * REDHAT: RHSA-2011:0887
<http://www.redhat.com/support/errata/RHSA-2011-0887.html>
- * REDHAT: RHSA-2011:0888
<http://www.redhat.com/support/errata/RHSA-2011-0888.html>
- * SUSE: SUSE-SA:2011:028
<http://lists.opensuse.org/opensuse-security-announce/2011-07/msg00001.html>

CVE Reference:

CVE-2011-2364 (cve.mitre.org, nvd.nist.gov)

• 19476 Mozilla Firefox - Miscellaneous memory safety hazards (CVE-2011-2365) (Remote File Checking)

Unspecified vulnerability in the browser engine in Mozilla Firefox 3.6.x before 3.6.18 and Thunderbird before 3.1.11 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-2364.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-19.html>
- * CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=655742
- * DEBIAN: DSA-2268
<http://www.debian.org/security/2011/dsa-2268>
- * DEBIAN: DSA-2269
<http://www.debian.org/security/2011/dsa-2269>
- * DEBIAN: DSA-2273
<http://www.debian.org/security/2011/dsa-2273>
- * MANDRIVA: MDVSA-2011:111
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:111>
- * REDHAT: RHSA-2011:0885
<http://www.redhat.com/support/errata/RHSA-2011-0885.html>
- * REDHAT: RHSA-2011:0886
<http://www.redhat.com/support/errata/RHSA-2011-0886.html>
- * REDHAT: RHSA-2011:0887
<http://www.redhat.com/support/errata/RHSA-2011-0887.html>
- * REDHAT: RHSA-2011:0888
<http://www.redhat.com/support/errata/RHSA-2011-0888.html>
- * SUSE: SUSE-SA:2011:028
<http://lists.opensuse.org/opensuse-security-announce/2011-07/msg00001.html>

CVE Reference:

CVE-2011-2365 (cve.mitre.org, nvd.nist.gov)

• 19477 Mozilla Firefox - Use-after-free vulnerability when viewing XUL document with script disabled (Remote File Checking)

Use-after-free vulnerability in Mozilla Firefox before 3.6.18 and 4.x through 4.0.1, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14, when JavaScript is disabled, allows remote attackers to execute arbitrary code via a crafted XUL document.

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

References:

- * CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-20.html>

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=617247
* DEBIAN: DSA-2268
<http://www.debian.org/security/2011/dsa-2268>
* DEBIAN: DSA-2269
<http://www.debian.org/security/2011/dsa-2269>
* DEBIAN: DSA-2273
<http://www.debian.org/security/2011/dsa-2273>
* MANDRIVA: MDVSA-2011:111
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:111>
* REDHAT: RHSA-2011:0885
<http://www.redhat.com/support/errata/RHSA-2011-0885.html>
* REDHAT: RHSA-2011:0887
<http://www.redhat.com/support/errata/RHSA-2011-0887.html>
* REDHAT: RHSA-2011:0888
<http://www.redhat.com/support/errata/RHSA-2011-0888.html>
* SUSE: SUSE-SA:2011:028
<http://lists.opensuse.org/opensuse-security-announce/2011-07/msg00001.html>

CVE Reference:

CVE-2011-2373 (cve.mitre.org, nvd.nist.gov)

• 19478 Mozilla Firefox - Memory corruption due to multipart/x-mixed-replace images (Remote File Checking)

Mozilla Firefox before 3.6.18 and 4.x through 4.0.1, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a multipart/x-mixed-replace image.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-21.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=638018
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=639303
* MANDRIVA: MDVSA-2011:111
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:111>
* REDHAT: RHSA-2011:0885
<http://www.redhat.com/support/errata/RHSA-2011-0885.html>
* REDHAT: RHSA-2011:0886
<http://www.redhat.com/support/errata/RHSA-2011-0886.html>
* REDHAT: RHSA-2011:0887
<http://www.redhat.com/support/errata/RHSA-2011-0887.html>
* REDHAT: RHSA-2011:0888
<http://www.redhat.com/support/errata/RHSA-2011-0888.html>
* SUSE: SUSE-SA:2011:028
<http://lists.opensuse.org/opensuse-security-announce/2011-07/msg00001.html>

CVE Reference:

CVE-2011-2377 (cve.mitre.org, nvd.nist.gov)

• 19479 Mozilla Firefox - Integer overflow and arbitrary code execution in Array.reduceRight() (Remote File Checking)

Integer overflow in the Array.reduceRight method in Mozilla Firefox before 3.6.18 and 4.x through 4.0.1, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14 allows remote attackers to execute arbitrary code via vectors involving a long JavaScript Array object.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2011/mfsa2011-22.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=664009
* DEBIAN: DSA-2268

<http://www.debian.org/security/2011/dsa-2268>

* DEBIAN: DSA-2269

<http://www.debian.org/security/2011/dsa-2269>

* DEBIAN: DSA-2273

<http://www.debian.org/security/2011/dsa-2273>

* MANDRIVA: MDVSA-2011:111

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:111>

* REDHAT: RHSA-2011:0885

<http://www.redhat.com/support/errata/RHSA-2011-0885.html>

* REDHAT: RHSA-2011:0887

<http://www.redhat.com/support/errata/RHSA-2011-0887.html>

* REDHAT: RHSA-2011:0888

<http://www.redhat.com/support/errata/RHSA-2011-0888.html>

* SUSE: SUSE-SA:2011:028

<http://lists.opensuse.org/opensuse-security-announce/2011-07/msg00001.html>

CVE Reference:

CVE-2011-2371 (cve.mitre.org, nvd.nist.gov)

• 19480 Mozilla Firefox - Stealing of cross-domain images using WebGL textures (Remote File Checking)

Mozilla Gecko before 5.0, as used in Firefox before 5.0 and Thunderbird before 5.0, does not block use of a cross-domain image as a WebGL texture, which allows remote attackers to obtain approximate copies of arbitrary images via a timing attack involving a crafted WebGL fragment shader.

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

References:

* MLIST: [whatwg] 20110314 Canvas and drawWindow

<http://lists.whatwg.org/pipermail/whatwg-whatwg.org/2011-March/030882.html>

* MISC:

<http://www.contextis.co.uk/resources/blog/webgl/>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=655987

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=656277

* CONFIRM:

https://developer.mozilla.org/en/WebGL/Cross-Domain_Textures

* CONFIRM:

<https://hacks.mozilla.org/2011/06/cross-domain-webgl-textures-disabled-in-firefox-5/>

* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-25.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=659349

* SUSE: SUSE-SA:2011:028

<http://lists.opensuse.org/opensuse-security-announce/2011-07/msg00001.html>

CVE Reference:

CVE-2011-2366 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-3348 Apache CVSS 2.0 Score = 4.3

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/69804>

SECTRACK: <http://www.securitytracker.com/id?1026054>

BID: <http://www.securityfocus.com/bid/49616>

CONFIRM: <http://www.apache.org/dist/httpd/Announcement2.2.html>

SECUNIA: <http://secunia.com/advisories/46013>

CONFIRM: http://httpd.apache.org/security/vulnerabilities_22.html#2.2.21

CVE Reference: [CVE-2011-3348](#)

• **CVE-2011-2412 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP Business Service Automation (BSA) Essentials 2.01 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=131645943904951&w=2>

HP: <http://marc.info/?l=bugtraq&m=131645943904951&w=2>

CVE Reference: [CVE-2011-2412](#)

• **CVE-2011-3577 IBM CVSS 2.0 Score = 10.0**

IBM WebSphere Commerce 6.x through 6.0.0.11 and 7.x through 7.0.0.3 does not properly implement Activity Token authentication for Web Services, which has unspecified impact and attack vectors.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/69838>

BID: <http://www.securityfocus.com/bid/49643>

OSVDB: <http://www.osvdb.org/75428>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg24030908>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1JR40420>

SECUNIA: <http://secunia.com/advisories/45999>

CVE Reference: [CVE-2011-3577](#)

• **CVE-2011-3575 IBM CVSS 2.0 Score = 9.0**

Stack-based buffer overflow in the NSFComputeEvaluateExt function in Nnotes.dll in IBM Lotus Domino 8.5.2 allows remote authenticated users to execute arbitrary code via a long tHPRAgentName parameter in an fmHttpPostRequest OpenForm action to WebAdmin.nsf.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/69802>

BID: <http://www.securityfocus.com/bid/49705>

MISC: <http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211>

MISC: http://www.research.reversingcode.com/exploits/IBMLotusDomino_StackOverflowPoC

CVE Reference: [CVE-2011-3575](#)

• **CVE-2011-2738 Cisco CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in Cisco Unified Service Monitor before 8.6, as used in Unified Operations Manager before 8.6 and CiscoWorks LAN Management Solution 3.x and 4.x before 4.1; and multiple EMC Ionix products including Application Connectivity Monitor (Ionix ACM) 2.3 and earlier, Adapter for Alcatel-Lucent 5620 SAM EMS (Ionix ASAM) 3.2.0.2 and earlier, IP Management Suite (Ionix IP) 8.1.1.1 and earlier, and other Ionix products; allow remote attackers to execute arbitrary code via crafted packets to TCP port 9002, aka Bug IDs CSCtn42961 and CSCtn64922, related to a buffer overflow.

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

References:

SECTRAK: <http://www.securitytracker.com/id?1026059>

BID: <http://www.securityfocus.com/bid/49644>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/519646/100/0/threaded>

OSVDB: <http://www.osvdb.org/75442>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b9351f.shtml

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b9351e.shtml

SECUNIA: <http://secunia.com/advisories/46053>

SECUNIA: <http://secunia.com/advisories/46016>

SECUNIA: <http://secunia.com/advisories/45979>

CVE Reference: [CVE-2011-2738](#)

• **CVE-2011-3290 Cisco CVSS 2.0 Score = 10.0**

Cisco Identity Services Engine (ISE) before 1.0.4.MR2 has default Oracle database credentials, which allows remote attackers to modify settings or perform unspecified other administrative actions via unknown vectors, aka Bug ID CSCts59135.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b95105.shtml

CVE Reference: [CVE-2011-3290](#)

• **CVE-2011-2543 Cisco CVSS 2.0 Score = 9.0**

Buffer overflow in the cuil component in Cisco Telepresence System Integrator C Series 4.x before TC4.2.0 allows remote authenticated users to cause a denial of service (endpoint reboot or process crash) or possibly execute arbitrary code via a long location parameter to the getxml program, aka Bug ID CSCtq46496.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/69907>

BID: <http://www.securityfocus.com/bid/49670>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/519698/100/0/threaded>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/17871>

SECTRAK: <http://securitytracker.com/id?1026072>

SECUNIA: <http://secunia.com/advisories/46109>

SECUNIA: <http://secunia.com/advisories/46057>

CVE Reference: [CVE-2011-2543](#)

• **CVE-2011-2430 Adobe CVSS 2.0 Score = 9.3**

Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows remote attackers to execute arbitrary code via crafted streaming media, related to a "logic error vulnerability."

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

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb11-26.html>

CVE Reference: [CVE-2011-2430](#)

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