

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

PCI council enforces standards by revoking company's QSA status. AntiSec posts stolen police data. Microsoft fixing 22 vulnerabilities. Also updates from Adobe.

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

• PCI Council revokes company's QSA status

Merchants that use Scottsdale, Ariz.-based security services provider Chief Security Officers (CSO) to validate their adherence with the Payment Card Industry Data Security Standard (PCI DSS) will have to find a new assessor. The PCI Security Standards Council, the group responsible for managing payment security, last week revoked CSO's status as a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA). CSO was removed from the Council's lists of approved service providers due to its "failure to satisfy the high standard set forth for QSAs and PA-QSAs," the PCI Council said in a statement released last week.

The PCI Council has not revealed why exactly CSO's credentials were revoked. CSO, meanwhile, did not respond to several interview requests made by SCMagazineUS.com. SC Magazine

Full Story :

http://www.scmagazineus.com/pci-council-revokes-companys-qa-status/article/209309/?utm_source=feedburner&u

• AntiSec hackers release cache of police data

Members of the AntiSec movement over the weekend released a cache of data belonging to law enforcement bodies across the United States in retaliation for recent hacking arrests. The leak, dubbed "Shooting Sheriffs Saturday," contains more than 10 GB of stolen data belonging to sheriff's offices for mostly rural towns across the country, according to a statement the hackers posted Saturday to the file-sharing site Pastebin. The data dump includes private emails, passwords, addresses, Social Security numbers, credit card numbers, police training files, and information from informants.

The hack was part of a venture called Anti-Security, or AntiSec, which is led by the hacktivist groups Anonymous and LulzSec, and calls for hackers worldwide to expose sensitive data that reveals wrongdoing within governments and corporations. SC Magazine

Full Story :

http://www.scmagazineus.com/antisechackers-release-cache-of-police-data/article/209253/?utm_source=feedburner

• Microsoft Patch Tuesday fixes 22 vulnerabilities

As part of its monthly Patch Tuesday upgrades, Microsoft on Tuesday released fixes for 22 vulnerabilities discovered in Internet Explorer, Windows, Visio and Visual Studio.

As previously mentioned, Microsoft released 13 security bulletins, two of which are rated critical in severity, nine important and two moderate.

The Redmond, Wash.-based company advised customers to install all of the updates as soon as possible, starting with the two rated most critical. SC Magazine

Full Story :

http://www.scmagazineus.com/microsoft-patch-tuesday-fixes-22-vulnerabilities/article/209324/?utm_source=feedburner

• Adobe issues critical updates for Flash, Shockwave

On the heels of a large Patch Tuesday load from Microsoft, Adobe on Tuesday released a slew of security updates affecting several of its products. "Critical" updates were released for Flash Player, Flash Media Server, Shockwave Player and Photoshop CS5. In addition, an "important" update was released for Adobe's help-authoring tool RoboHelp.

Adobe said it is not aware of any in-the-wild exploits targeting any of the issues addressed in its updates Tuesday.

The Flash Player update is the largest of the lot, addressing 13 critical flaws that could cause a crash or allow an attacker to take control of an affected system, Adobe said in its release. The fix addresses issues in version 10.3.181.36 and earlier editions for Windows, Mac, Linux and Solaris operating systems, as well as version 10.3.185.25 and earlier for Android and Adobe AIR 2.7. SC Magazine

Full Story :

http://www.scmagazineus.com/adobe-issues-critical-updates-for-flash-shockwave/article/209372/?utm_source=feedburner

New Vulnerabilities Tested in SecureScout

• 13815 Oracle Database Server - EMCTL component unspecified Vulnerability (jul-2011/CVE-2011-0881)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>

* SECTRAK: 1025795

<http://www.securitytracker.com/id/1025795>

* BID: 48736

<http://www.securityfocus.com/bid/48736>

* SECUNIA: 45274

<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-0881 (cve.mitre.org, nvd.nist.gov)

• 13816 Oracle Database Server - Enterprise Manager Console component unspecified Vulnerability (jul-2011/CVE-2011-0876)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Enterprise Manager Console" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>
- * SECTRACK: 1025795
<http://www.securitytracker.com/id/1025795>
- * BID: 48737
<http://www.securityfocus.com/bid/48737>
- * SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-0876 (cve.mitre.org, nvd.nist.gov)

• **13817 Oracle Database Server - Event Management component unspecified Vulnerability (jul-2011/CVE-2011-0830)**

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>
- * SECTRACK: 1025795
<http://www.securitytracker.com/id/1025795>
- * BID: 48740
<http://www.securityfocus.com/bid/48740>
- * SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-0830 (cve.mitre.org, nvd.nist.gov)

• **13818 Oracle Database Server - Instance Management component unspecified Vulnerability (jul-2011/CVE-2011-0877)**

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>
- * SECTRACK: 1025795
<http://www.securitytracker.com/id/1025795>
- * BID: 48741
<http://www.securityfocus.com/bid/48741>
- * SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-0877 (cve.mitre.org, nvd.nist.gov)

• **13819 Oracle Database Server - Instance Management component unspecified Vulnerability (jul-2011/CVE-2011-0879)**

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

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

References:

* CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>
* SECTRACK: 1025795
<http://www.securitytracker.com/id/1025795>
* BID: 48745
<http://www.securityfocus.com/bid/48745>
* SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-0879 (cve.mitre.org, nvd.nist.gov)

• **13820 Oracle Database Server - XML Developer Kit component unspecified Vulnerability (jul-2011/CVE-2011-2231)**

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

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

References:

* CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>
* SECTRACK: 1025795
<http://www.securitytracker.com/id/1025795>
* BID: 48746
<http://www.securityfocus.com/bid/48746>
* SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-2231 (cve.mitre.org, nvd.nist.gov)

• **13821 Oracle Database Server - Database Vault component unspecified Vulnerability (jul-2011/CVE-2011-2238)**

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

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

References:

* CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>
* SECTRACK: 1025795
<http://www.securitytracker.com/id/1025795>
* BID: 48754
<http://www.securityfocus.com/bid/48754>
* SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-2238 (cve.mitre.org, nvd.nist.gov)

• **13822 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2011/CVE-2011-2243)**

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

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

References:

* CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>
* SECTRACK: 1025795
<http://www.securitytracker.com/id/1025795>
* BID: 48764
<http://www.securityfocus.com/bid/48764>
* SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-2243 (cve.mitre.org, nvd.nist.gov)

• **13823 Oracle Database Server - Oracle Universal Installer component unspecified Vulnerability (jul-2011/CVE-2011-2240)**

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

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

References:

* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>

* SECTRACK: 1025795

<http://www.securitytracker.com/id/1025795>

* BID: 48749

<http://www.securityfocus.com/bid/48749>

* SECUNIA: 45274

<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-2240 (cve.mitre.org, nvd.nist.gov)

• **13824 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2011/CVE-2011-2242)**

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

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

References:

* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>

* SECTRACK: 1025795

<http://www.securitytracker.com/id/1025795>

* BID: 48750

<http://www.securityfocus.com/bid/48750>

* SECUNIA: 45274

<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-2242 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2011-1966 Microsoft CVSS 2.0 Score = 10.0**

The DNS server in Microsoft Windows Server 2008 SP2, R2, and R2 SP1 does not properly handle NAPTR queries that trigger recursive processing, which allows remote attackers to execute arbitrary code via a crafted query, aka "DNS NAPTR Query Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-058.mspx>

CVE Reference: [CVE-2011-1966](http://cve.mitre.org)

• **CVE-2011-1979 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Visio 2003 SP3 and 2007 SP2 does not properly validate objects in memory during Visio file parsing, which allows remote attackers to execute arbitrary code via a crafted file, aka "Move Around the Block RCE Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-060.mspx>

CVE Reference: [CVE-2011-1979](#)

• **CVE-2011-1972 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Visio 2003 SP3, 2007 SP2, and 2010 Gold and SP1 does not properly validate objects in memory during Visio file parsing, which allows remote attackers to execute arbitrary code via a crafted file, aka "pStream Release RCE Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-060.msp>

CVE Reference: [CVE-2011-1972](#)

• **CVE-2011-1964 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, aka "Style Object Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-057.msp>

CVE Reference: [CVE-2011-1964](#)

• **CVE-2011-1961 Microsoft CVSS 2.0 Score = 9.3**

The telnet URI handler in Microsoft Internet Explorer 6 through 9 does not properly launch the handler application, which allows remote attackers to execute arbitrary programs via a crafted web site, aka "Telnet Handler Remote Code Execution Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-057.msp>

CVE Reference: [CVE-2011-1961](#)

• **CVE-2011-1963 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 7 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, aka "XSLT Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-057.msp>

CVE Reference: [CVE-2011-1963](#)

• **CVE-2011-1975 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in the Data Access Tracing component in Windows Data Access Components (Windows DAC) 6.0 in Microsoft Windows 7 Gold and SP1 and Windows Server 2008 R2 and R2 SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains an Excel .xlsx file, aka "Data Access Components 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/MS11-059.msp>

CVE Reference: [CVE-2011-1975](#)

• **CVE-2011-1871 Microsoft CVSS 2.0 Score = 7.8**

Tcpip.sys in the TCP/IP stack in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (reboot) via a series of crafted ICMP

messages, aka "ICMP Denial of Service Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-064.msp>

CVE Reference: [CVE-2011-1871](#)

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