

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

Web applications under constant attack. Anonymous angry with PayPal and FBI. Website listing Cloud vendors security controls on the way. US voting for mandatory ISP log-keeping.

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

• Web apps attacked every two minutes, says study

The average Web-based application is hit by a cyberattack once every two minutes, says a report out today by security firm Imperva.

Detailing its findings in its "Web Application Attack Report" (PDF) for July, Imperva found that Web applications are attacked around 27 times per hour. Monitoring the Internet from December 2010 through May 2011, the security firm uncovered and categorized more than 10 million individual attacks targeting both business and government sites.

Automated cyberattacks accounted for a huge number of attempted breaches. The report discovered that attack traffic was characterized by quick spikes of high volumes followed by longer periods of lighter activity, a key factor pointing to automation. Further, Web sites hit by automated attacks on average received up to 25,000 such attacks in just one hour, or seven attacks each second. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20083576-83/web-apps-attacked-every-two-minutes-study-finds/?part=rss&subj=

• Anonymous urges PayPal boycott, condemns FBI

Anonymous is lashing out today at the FBI and especially at PayPal, urging users of the electronic payments site to dump their accounts.

In its latest "official communique" on behalf of itself and Lulz Security, the hactivist group condemned the FBI for its recent arrests of those charged in connection with hacking attacks by Anonymous in December against PayPal and a host of other companies.

Complaining that the Anonymous "suspects" may face a fine of \$500,000 and a possible 15 years of jail time, the group criticized the FBI for equating "adding one's voice to a chorus" with "controlling a large botnet of infected computers" and charging both as crimes subject to the same fines and sentences. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20084171-83/anonymous-urges-paypal-boycott-condemns-fbi/?part=rss&subj=new

• Nonprofit will publish how providers secure cloud

Soon anyone may only be a few clicks away from learning whether a cloud provider is up to snuff when it comes to security.

The nonprofit Cloud Security Alliance (CSA) is planning to develop and maintain on its website a public registry documenting the security controls that exist in various cloud computing offerings.

The repository, to be called CSA Security, Trust & Assurance Registry (STAR), will help cloud users assess the security of potential and existing providers, Jim Reavis, executive director of the CSA, told SCMagazineUS.com on Thursday. SC Magazine

Full Story :

http://www.scmagazineus.com/nonprofit-will-publish-how-providers-secure-cloud/article/208589/?utm_source=feed

• House panel approves broadened ISP snooping bill

Internet providers would be forced to keep logs of their customers' activities for one year--in case police want to review them in the future--under legislation that a U.S. House of Representatives committee approved today.

The 19 to 10 vote represents a victory for conservative Republicans, who made data retention their first major technology initiative after last fall's elections, and the Justice Department officials who have quietly lobbied for the sweeping new requirements, a development first reported by CNET.

House Judiciary committee prepares to vote on sweeping data retention mandate. Cnet Security

Full Story :

http://news.cnet.com/8301-31921_3-20084939-281/house-panel-approves-broadened-isp-snooping-bill/?part=rss&subj=new

New Vulnerabilities Tested in SecureScout

• 13795 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2011/CVE-2011-2239)

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

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

References:

* CONFIRM:

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

* SECTRACK: 1025795

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

* BID: 48726

<http://www.securityfocus.com/bid/48726>

* SECUNIA: 45274

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

CVE Reference:

CVE-2011-2239 (cve.mitre.org, nvd.nist.gov)

• 13796 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2011/CVE-2011-2253)

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>
- * SECTRACK: 1025795
<http://www.securitytracker.com/id/1025795>
- * BID: 48728
<http://www.securityfocus.com/bid/48728>
- * SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-2253 (cve.mitre.org, nvd.nist.gov)

• **13797 Oracle Database Server - Content Management component unspecified Vulnerability (jul-2011/CVE-2011-0882)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Content 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: 48732
<http://www.securityfocus.com/bid/48732>
- * SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-0882 (cve.mitre.org, nvd.nist.gov)

• **13798 Oracle Database Server - Database Target Type Menus component unspecified Vulnerability (jul-2011/CVE-2011-2257)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Database Target Type Menus" 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: 48751
<http://www.securityfocus.com/bid/48751>
- * SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-2257 (cve.mitre.org, nvd.nist.gov)

• **13799 Oracle Database Server - SQL Performance Advisories/UIs component unspecified Vulnerability (jul-2011/CVE-2011-2248)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "SQL Performance Advisories/UIs" 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: 48729
<http://www.securityfocus.com/bid/48729>
* SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-2248 (cve.mitre.org, nvd.nist.gov)

• **13800 Oracle Database Server - Schema Management component unspecified Vulnerability (jul-2011/CVE-2011-0870)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Schema 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: 48146
<http://www.securityfocus.com/bid/48146>
* SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-0870 (cve.mitre.org, nvd.nist.gov)

• **13801 Oracle Database Server - Security Framework component unspecified Vulnerability (jul-2011/CVE-2011-0848)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Security Framework" 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: 48739
<http://www.securityfocus.com/bid/48739>
* SECUNIA: 45274
<http://secunia.com/advisories/45274/>

CVE Reference:

CVE-2011-0848 (cve.mitre.org, nvd.nist.gov)

• **13802 Oracle Database Server -Security Management component unspecified Vulnerability (jul-2011/CVE-2011-0852)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Security 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: 48734
<http://www.securityfocus.com/bid/48734>
* SECUNIA: 45274

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

CVE Reference:

CVE-2011-0852 (cve.mitre.org, nvd.nist.gov)

• **13803 Oracle Database Server - Streams, AQ & Replication Mgmt component unspecified Vulnerability (jul-2011/CVE-2011-0822)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Streams, AQ & Replication Mgmt" 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: 48137

<http://www.securityfocus.com/bid/48137>

* SECUNIA: 45274

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

CVE Reference:

CVE-2011-0822 (cve.mitre.org, nvd.nist.gov)

• **13804 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2011/CVE-2011-0835)**

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>

* SECTRAK: 1025795

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

* BID: 48727

<http://www.securityfocus.com/bid/48727>

* SECUNIA: 45274

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

CVE Reference:

CVE-2011-0835 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2011-2884 IBM CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in IBM Lotus Symphony 3 before FP3 have unknown impact and attack vectors, related to "critical security vulnerability issues."

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

References:

CONFIRM:

https://www-304.ibm.com/jct03001c/software/lotus/symphony/idcontents/releasenotes/en/readme_embedded_in_fixpack3

OSVDB: <http://www.osvdb.org/73988>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21505448>

CONFIRM:

http://www.ibm.com/software/lotus/symphony/idcontents/releasenotes/en/readme_fixpack3_standalone_long.htm

CONFIRM:

http://www.ibm.com/software/lotus/symphony/buzz.nsf/web_DisplayPlugin?open&unid=9717F6F587AAA939852578D300

SECUNIA: <http://secunia.com/advisories/45271>

CVE Reference: [CVE-2011-2884](#)

• **CVE-2011-2893 IBM CVSS 2.0 Score = 4.3**

The DataPilot feature in IBM Lotus Symphony 3 before FP3 allows user-assisted remote attackers to cause a denial of service (application crash) via a large .xls spreadsheet with an invalid Value reference.

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

References:

CONFIRM:

https://www-304.ibm.com/jct03001c/software/lotus/symphony/idcontents/releasenotes/en/readme_embedded_in_fixpack3

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21505448>

CONFIRM:

http://www.ibm.com/software/lotus/symphony/idcontents/releasenotes/en/readme_fixpack3_standalone_long.htm

CONFIRM:

http://www.ibm.com/software/lotus/symphony/buzz.nsf/web_DisplayPlugin?open&unid=9717F6F587AAA939852578D300

CVE Reference: [CVE-2011-2893](#)

• **CVE-2011-2888 IBM CVSS 2.0 Score = 4.3**

IBM Lotus Symphony 3 before FP3 allows remote attackers to cause a denial of service (application hang) via complex graphics in a presentation.

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

References:

CONFIRM:

https://www-304.ibm.com/jct03001c/software/lotus/symphony/idcontents/releasenotes/en/readme_embedded_in_fixpack3

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21505448>

CONFIRM:

http://www.ibm.com/software/lotus/symphony/idcontents/releasenotes/en/readme_fixpack3_standalone_long.htm

CONFIRM:

http://www.ibm.com/software/lotus/symphony/buzz.nsf/web_DisplayPlugin?open&unid=9717F6F587AAA939852578D300

CVE Reference: [CVE-2011-2888](#)

• **CVE-2011-2886 IBM CVSS 2.0 Score = 4.3**

IBM Lotus Symphony 3 before FP3 allows remote attackers to cause a denial of service (application crash) via a .docx document with empty bullet styles for parent bullets.

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

References:

CONFIRM:

https://www-304.ibm.com/jct03001c/software/lotus/symphony/idcontents/releasenotes/en/readme_embedded_in_fixpack3

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21505448>

CONFIRM:

http://www.ibm.com/software/lotus/symphony/idcontents/releasenotes/en/readme_fixpack3_standalone_long.htm

CONFIRM:

http://www.ibm.com/software/lotus/symphony/buzz.nsf/web_DisplayPlugin?open&unid=9717F6F587AAA939852578D300

CVE Reference: [CVE-2011-2886](#)

• **CVE-2011-2887 IBM CVSS 2.0 Score = 4.3**

IBM Lotus Symphony 3 before FP3 on Linux allows remote attackers to cause a denial of service (application crash) via a certain sample document.

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

References:

CONFIRM:

https://www-304.ibm.com/jct03001c/software/lotus/symphony/idcontents/releasenotes/en/readme_embedded_in_fixpack3

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21505448>

CONFIRM:

http://www.ibm.com/software/lotus/symphony/idcontents/releasenotes/en/readme_fixpack3_standalone_long.htm

CONFIRM:

http://www.ibm.com/software/lotus/symphony/buzz.nsf/web_DisplayPlugin?open&unid=9717F6F587AAA939852578D300

CVE Reference: [CVE-2011-2887](#)

• **CVE-2011-2885 IBM CVSS 2.0 Score = 4.3**

IBM Lotus Symphony 3 before FP3 allows remote attackers to cause a denial of service (application crash) via the sample .doc document that incorporates a user-defined toolbar.

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

References:

CONFIRM:

https://www-304.ibm.com/jct03001c/software/lotus/symphony/idcontents/releasenotes/en/readme_embedded_in_fixpack3

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21505448>

CONFIRM:

http://www.ibm.com/software/lotus/symphony/idcontents/releasenotes/en/readme_fixpack3_standalone_long.htm

CONFIRM:

http://www.ibm.com/software/lotus/symphony/buzz.nsf/web_DisplayPlugin?open&unid=9717F6F587AAA939852578D300

CVE Reference: [CVE-2011-2885](#)

• **CVE-2011-1829 Debian CVSS 2.0 Score = 4.3**

APT before 0.8.15.2 does not properly validate inline GPG signatures, which allows man-in-the-middle attackers to install modified packages via vectors involving lack of an initial clearsigned message.

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

References:

CONFIRM: <https://launchpad.net/ubuntu/+archive/primary/+sourcepub/1817196/+listing-archive-extra>

CONFIRM: http://launchpadlibrarian.net/75126628/apt_0.8.13.2ubuntu2_0.8.13.2ubuntu4.1.diff.gz

CONFIRM: <https://launchpad.net/bugs/784473>

XF: <http://xforce.iss.net/xforce/xfdb/68560>

UBUNTU: <http://www.ubuntu.com/usn/USN-1169-1>

BID: <http://www.securityfocus.com/bid/48671>

CONFIRM: <http://packages.debian.org/changelogs/pool/main/a/apt/current/changelog>

CVE Reference: [CVE-2011-1829](#)

• **CVE-2011-2196 redhat CVSS 2.0 Score = 6.8**

jboss-seam.jar in the JBoss Seam 2 framework 2.2.x and earlier, as distributed in Red Hat JBoss Enterprise SOA Platform 4.3.0.CP05 and 5.1.0; JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.3.0, 4.3.0.CP09, and 5.1.1; and JBoss Enterprise Web Platform 5.1.1, does not properly restrict use of Expression Language (EL) statements in FacesMessages during page exception handling, which allows remote attackers to execute arbitrary Java code via a crafted URL to an application. NOTE: this vulnerability exists because of an incomplete fix for

CVE-2011-1484.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=712283

BID: <http://www.securityfocus.com/bid/48716>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0952.html>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0951.html>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0950.html>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0949.html>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0948.html>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0947.html>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0946.html>

REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0945.html>

CVE Reference: [CVE-2011-2196](#)

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