

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

Mobile big in big business. Cookiejacking possible in IE. The Sony disaster continues to unfold. RSA attack may cause problems for defense contractor.

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

• Risky mobile behaviors routine in business

Like it or not, iPads, iPhones and Android devices are making their way into enterprises, and while a vast majority of organizations have policies around mobile device use, risky behaviors are still commonplace, according to a report released Tuesday by McAfee and Carnegie Mellon University. The report, which focused on the consumerization of IT and its impact on security, found that there is a "serious disconnect" between policy and reality in the mobile computing environment within the enterprise. A survey of more than 1,500 mobile device end-users and senior IT decision-makers, conducted by research firm Vanson Bourne, on behalf of McAfee and Carnegie Mellon, found that 95 percent of organizations have mobile security policies in place. Only one in three employees are very aware of such policies, however.

"This means that unmanaged and unsecured devices predominate, even as the mobile device population continues to grow," David Goldschalg, vice president of mobility at McAfee, told SCMagazineUS.com in an email Wednesday. sc Magazine

Full Story :

• Security researcher finds 'cookiejacking' risk in IE

A security researcher in Italy has discovered a flaw in Internet Explorer that he says could enable hackers to steal cookies from a PC and then log onto password-protected Web sites.

Referring to the exploit as "cookiejacking," Rosario Valotta claims that a zero-day vulnerability found in every version of Microsoft's IE under any version of Windows allows an attacker to hijack any cookie for any Web site.

Demonstrating his findings at security conferences this month in Switzerland and Amsterdam, Valotta acknowledges that to exploit the hole, the hacker must employ a bit of social engineering because the victim must drag and drop an object across the PC for the cookie to be stolen. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20066419-83.html?part=rss&subj=news&tag=2547-1_3-0-20

• Report: Sony Music Japan, Sony Ericsson hacked

The onslaught against Sony apparently continues: this time hackers have targeted Sony Music Entertainment Japan and stolen information from thousands of accounts in a Canadian Sony Ericsson eShop site, a spokesperson confirmed today.

Meanwhile, e-mails, phone numbers, and passwords of more than 8,000 accounts at Sony Music Greece were stolen over the weekend, Sony confirmed. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20065816-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Report: Lockheed Martin fighting off network attack

The major defense contractor Lockheed Martin is experiencing a massive network disruption that may be related to an attack on RSA earlier this year in which information about the security company's two-factor authentication offerings was compromised.

According to a Reuters report, citing two unnamed sources, the network problems are impacting many people.

The incident was first brought to light Wednesday by technology blogger Robert Cringely, who noted that a "very large U.S. defense contractor" was forced to cut off remote access to its internal network following a compromise. As a result, the company is being forced to replace RSA SecurID tokens and mandate password resets for more than 100,000 users. SC Magazine

Full Story :

http://www.scmagazineus.com/report-lockheed-martin-fighting-off-network-attack/article/204002/?utm_source=feedburner&

New Vulnerabilities Tested in SecureScout

• 13786 Oracle Database Server - Oracle Warehouse Builder component unspecified Vulnerability (apr-2011/CVE-2011-0792)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

* BID: 47429

<http://www.securityfocus.com/bid/47429>

* SECTRACK: 1025391

<http://www.securitytracker.com/id/1025391>

CVE Reference:

CVE-2011-0792 (cve.mitre.org, nvd.nist.gov)

• 13787 Oracle Database Server - Oracle Warehouse Builder component unspecified Vulnerability (apr-2011/CVE-2011-0799)

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>
- * BID: 47431
<http://www.securityfocus.com/bid/47431>
- * SECTRACK: 1025391
<http://www.securitytracker.com/id/1025391>

CVE Reference:

CVE-2011-0799 (cve.mitre.org, nvd.nist.gov)

● **13788 Oracle Database Server - Oracle Security Service component unspecified Vulnerability (apr-2011/CVE-2009-3555)**

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>
- * BID: 36935
<http://www.securityfocus.com/bid/36935>
- * SECTRACK: 1025391
<http://www.securitytracker.com/id/1025391>

CVE Reference:

CVE-2009-3555 (cve.mitre.org, nvd.nist.gov)

● **13789 Oracle Database Server - Application Service Level Management component unspecified Vulnerability (apr-2011/CVE-2011-0787)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Application Service Level Management" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>
- * BID: 47451
<http://www.securityfocus.com/bid/47451>
- * SECTRACK: 1025391
<http://www.securitytracker.com/id/1025391>

CVE Reference:

CVE-2011-0787 (cve.mitre.org, nvd.nist.gov)

● **13790 Oracle Database Server - Network Foundation component unspecified Vulnerability (apr-2011/CVE-2011-0806)**

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>
- * BID: 47430
<http://www.securityfocus.com/bid/47430>
- * SECTRACK: 1025391
<http://www.securitytracker.com/id/1025391>

CVE Reference:

CVE-2011-0806 (cve.mitre.org, nvd.nist.gov)

• 13791 Oracle Database Server - Oracle Help component unspecified Vulnerability (apr-2011/CVE-2011-0785)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

* SECTRACK: 1025391

<http://www.securitytracker.com/id/1025391>

CVE Reference:

CVE-2011-0785 (cve.mitre.org, nvd.nist.gov)

• 13792 Oracle Database Server - UIX component unspecified Vulnerability (apr-2011/CVE-2011-0805)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

* SECTRACK: 1025391

<http://www.securitytracker.com/id/1025391>

* BID: 47441

<http://www.securityfocus.com/bid/47441>

CVE Reference:

CVE-2011-0805 (cve.mitre.org, nvd.nist.gov)

• 13793 Oracle Database Server - Database Vault component unspecified Vulnerability (apr-2011/CVE-2011-0793)

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/cpuapr2011-301950.html>

* SECTRACK: 1025391

<http://www.securitytracker.com/id/1025391>

* BID: 47436

<http://www.securityfocus.com/bid/47436>

CVE Reference:

CVE-2011-0793 (cve.mitre.org, nvd.nist.gov)

• 13794 Oracle Database Server - Database Vault component unspecified Vulnerability (apr-2011/CVE-2011-0804)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

* SECTRACK: 1025391

<http://www.securitytracker.com/id/1025391>

* BID: 47432

<http://www.securityfocus.com/bid/47432>

CVE Reference:

CVE-2011-0804 (cve.mitre.org, nvd.nist.gov)

• 19340 Scripting Memory Reallocation Vulnerability (MS11-031/2514666) (Remote File Checking)

A remote code execution vulnerability exists in the JScript and VBScript scripting engines due to a memory corruption error. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the logged-on user. 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 / Gain Root** Risk: **High**

References:

- * MS: MS11-031
<http://www.microsoft.com/technet/security/Bulletin/MS11-031.msp>
- * BID: 47249
<http://www.securityfocus.com/bid/47249>
- * OSVDB: 71774
<http://osvdb.org/71774>
- * SECTRAK: 1025333
<http://www.securitytracker.com/id?1025333>
- * SECUNIA: 44162
<http://secunia.com/advisories/44162>
- * VUPEN: ADV-2011-0949
<http://www.vupen.com/english/advisories/2011/0949>

CVE Reference:

CVE-2011-0663 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-1928 Apache CVSS 2.0 Score = 4.3

The fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library 1.4.3 and 1.4.4, and the Apache HTTP Server 2.2.18, allows remote attackers to cause a denial of service (infinite loop) via a URI that does not match unspecified types of wildcard patterns, as demonstrated by attacks against mod_autoindex in httpd when a /*/WEB-INF/ configuration pattern is used. NOTE: this issue exists because of an incorrect fix for CVE-2011-0419.

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

References:

- MLIST: http://mail-archives.apache.org/mod_mbox/www-announce/201105.mbox/%3c4DD55076.1060005@apache.org%3e
- MLIST: http://mail-archives.apache.org/mod_mbox/httpd-announce/201105.mbox/%3C4DD55092.3030403@apache.org%3E
- CONFIRM: https://issues.apache.org/bugzilla/show_bug.cgi?id=51219
- VUPEN: <http://www.vupen.com/english/advisories/2011/1290>
- VUPEN: <http://www.vupen.com/english/advisories/2011/1289>
- SECUNIA: <http://secunia.com/advisories/44661>
- SECUNIA: <http://secunia.com/advisories/44558>
- MLIST: <http://openwall.com/lists/oss-security/2011/05/19/5>
- MLIST: <http://openwall.com/lists/oss-security/2011/05/19/10>
- CONFIRM: <http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=627182>

CVE Reference: [CVE-2011-1928](#)

• CVE-2011-2172 IBM CVSS 2.0 Score = 4.3

Cross-site scripting (XSS) vulnerability in the search center in IBM WebSphere Portal 7.0.0.1 before CF004 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/67594>

BID: <http://www.securityfocus.com/bid/47954>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg24029452>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM37009>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM36644>

SECUNIA: <http://secunia.com/advisories/44700>

CVE Reference: [CVE-2011-2172](#)

• **CVE-2011-2173 IBM CVSS 2.0 Score = 4.0**

The implementation of OutputMediator objects in IBM WebSphere Portal 6.0.1.7, and 7.0.0.1 before CF002, allows remote authenticated users to cause a denial of service (memory consumption) via requests.

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

References:

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg24029452>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM33432>

CVE Reference: [CVE-2011-2173](#)

• **CVE-2010-4806 IBM CVSS 2.0 Score = 4.0**

The authoring tool in IBM Web Content Manager (WCM) 6.1.5, and 7.0.0.1 before CF003, allows remote authenticated users to bypass intended access restrictions on draft creation by leveraging certain resource editor privileges.

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

References:

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg24029452>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM26755>

CVE Reference: [CVE-2010-4806](#)

• **CVE-2010-4807 IBM CVSS 2.0 Score = 3.5**

Race condition in IBM Web Content Manager (WCM) 7.0.0.1 before CF003 allows remote authenticated users to cause a denial of service (infinite recursive query) via unspecified vectors, related to a StackOverflowError exception.

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

References:

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg24029452>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM36141>

CVE Reference: [CVE-2010-4807](#)

• **CVE-2011-1804 Apple CVSS 2.0 Score = 7.5**

rendering/RenderBox.cpp in WebCore in WebKit before r86862, as used in Google Chrome before 11.0.696.71, does not properly render floats, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."

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

References:

CONFIRM: <http://trac.webkit.org/changeset/86862>

CONFIRM: <http://codereview.chromium.org/7050016>

CONFIRM: http://googlechromereleases.blogspot.com/2011/05/stable-channel-update_24.html

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=82546>

CVE Reference: [CVE-2011-1804](#)

• **CVE-2010-4251 Linux CVSS 2.0 Score = 6.1**

The socket implementation in net/core/sock.c in the Linux kernel before 2.6.34 does not properly manage a backlog of received packets, which allows remote attackers to cause a denial of service (memory consumption) by sending a large amount of network traffic, as demonstrated by netperf UDP tests.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=657303

MLIST: <http://kerneltrap.org/mailarchive/linux-netdev/2010/3/3/6271093/thread>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=8eae939f1400326b06d0c9afe53d2a484a326871>

BID: <http://www.securityfocus.com/bid/46637>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.34>

CVE Reference: [CVE-2010-4251](#)

• **CVE-2010-4805 Linux CVSS 2.0 Score = 6.1**

The socket implementation in net/core/sock.c in the Linux kernel before 2.6.35 does not properly manage a backlog of received packets, which allows remote attackers to cause a denial of service by sending a large amount of network traffic, related to the sk_add_backlog function and the sk_rmem_alloc socket field. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-4251.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=657303

MLIST: <http://kerneltrap.org/mailarchive/linux-netdev/2010/3/3/6271093/thread>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=c377411f2494a931ff7facdbb3a6839b1266bcf6>

BID: <http://www.securityfocus.com/bid/46637>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.35>

CVE Reference: [CVE-2010-4805](#)

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