

## 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

Now they can hack your car! US to monitor social networks. US to fund security research. Your laptop battery can be hacked.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netvigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • **Black Hat: Car unlocked, started via "war texting"**

At the Black Hat conference in Las Vegas on Wednesday, two researchers demonstrated how they were able to send commands via a laptop to unlock the doors of a Subaru Outback - and then, awing the audience, actually start the car.

Don Bailey and Matthew Solnik, security consultants at iSec Partners, used a technique they have dubbed "war texting" to tap into the system used to remotely control the car.

The researchers did not disclose the name of the affected system in order to give its manufacturer time to fix the issue.  
SC Magazine

Full Story :

[http://www.scmagazineus.com/black-hat-car-unlocked-started-via-war-texting/article/209037/?utm\\_source=feedburn](http://www.scmagazineus.com/black-hat-car-unlocked-started-via-war-texting/article/209037/?utm_source=feedburn)

### • **White House: Need to monitor online 'extremism'**

A White House terrorism strategy released today says Facebook, Twitter, and other social networks aid in "advancing violent extremist narratives" and should be monitored by the government.

The 12-page strategy (PDF), which outlines ways to respond to violent extremism, promises that: "We will continue to closely monitor the important role the Internet and social-networking sites play in advancing violent extremist narratives."

President Obama said in a statement accompanying the report that the federal government will start "helping communities to better understand and protect themselves against violent extremist propaganda, especially online."

Cnet Security

Full Story :

[http://news.cnet.com/8301-31921\\_3-20087677-281/white-house-need-to-monitor-online-extremism/?part=rss&subj=news](http://news.cnet.com/8301-31921_3-20087677-281/white-house-need-to-monitor-online-extremism/?part=rss&subj=news)

### • **Black Hat: New DARPA program to fund independent hackers**

Calling all independent security researchers: The government wants to fund your work.&nbsp;

As part of a new initiative, called Cyber Fast Track, described Thursday at the Black Hat&nbsp;conference in Las Vegas, the U.S. Defense Department will fund small hacker groups and independent researchers in the development of cutting-edge solutions that can be created in short intervals for a low cost.

The program is the brainchild of Peiter Zatko, a respected hacker known as "Mudge," who last February took on the role of program manager at the Defense Advanced Research Projects Agency (DARPA), the Defense Department's central research organization. SC Magazine

Full Story :

[http://www.scmagazineus.com/black-hat-new-darpa-program-to-fund-independent-hackers/article/209083/?utm\\_source=twitter](http://www.scmagazineus.com/black-hat-new-darpa-program-to-fund-independent-hackers/article/209083/?utm_source=twitter)

### • **Hacking laptop batteries: A new security threat**

Accuvant Labs' Charlie Miller describes how to hack Apple laptop batteries

(Credit: Declan McCullagh/CNET) LAS VEGAS--The latest security threat to your laptop comes from an unexpected source: its battery.

A security researcher demonstrated today at the Black Hat security conference how he was able to gain complete control of the microprocessor embedded in batteries used in Apple Macintosh laptops and then remove or bypass the built-in safeguards. Cnet Security

Full Story :

[http://news.cnet.com/8301-31921\\_3-20088290-281/hacking-laptop-batteries-a-new-security-threat/?part=rss&subj=news](http://news.cnet.com/8301-31921_3-20088290-281/hacking-laptop-batteries-a-new-security-threat/?part=rss&subj=news)

### • **Global cyber-espionage operation uncovered**

Shady RAT intrusions were rampant in 2008, the year of the Beijing Olympics. (Click image for a large, readable version.)

(Credit: McAfee) A widespread cyber-espionage campaign stole government secrets, sensitive corporate documents, and other intellectual property for five years from more than 70 public and private organizations in 14 countries, according to the McAfee researcher who uncovered the effort.

The campaign, dubbed "Operation Shady RAT" (RAT stands for "remote access tool") was discovered by Dmitri Alperovitch, vice president of threat research at the cyber-security firm McAfee. Vanity Fair's Michael Joseph Gross was first to write about the findings. The targets cut across industries, including government, defense, energy, electronics, media, real estate, agriculture, and construction. The governments hit include the U.S., Canada, South Korea, Vietnam, Taiwan, and India. Cnet Security

Full Story :

[http://news.cnet.com/8301-27080\\_3-20087268-245/global-cyber-espionage-operation-uncovered/?part=rss&subj=news](http://news.cnet.com/8301-27080_3-20087268-245/global-cyber-espionage-operation-uncovered/?part=rss&subj=news)

## **New Vulnerabilities Tested in SecureScout**

### • **13805 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2011/CVE-2011-0880)**

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: 48730  
<http://www.securityfocus.com/bid/48730>
- \* SECUNIA: 45274  
<http://secunia.com/advisories/45274/>

## CVE Reference:

CVE-2011-0880 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 13806 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2011/CVE-2011-0838)

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: 48731  
<http://www.securityfocus.com/bid/48731>
- \* SECUNIA: 45274  
<http://secunia.com/advisories/45274/>

## CVE Reference:

CVE-2011-0838 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 13807 Oracle Database Server - Security Framework component unspecified Vulnerability (jul-2011/CVE-2011-2244)

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: 48742  
<http://www.securityfocus.com/bid/48742>
- \* SECUNIA: 45274  
<http://secunia.com/advisories/45274/>

## CVE Reference:

CVE-2011-2244 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 13808 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2011/CVE-2011-0832)

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: 48748  
<http://www.securityfocus.com/bid/48748>
- \* SECUNIA: 45274  
<http://secunia.com/advisories/45274/>

**CVE Reference:**

CVE-2011-0832 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 13809 Oracle Database Server - XML Developer Kit component unspecified Vulnerability (jul-2011/CVE-2011-2232)**

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: 48755

<http://www.securityfocus.com/bid/48755>

\* SECUNIA: 45274

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

**CVE Reference:**

CVE-2011-2232 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 13810 Oracle Database Server - CMDB Metadata & Instance APIs component unspecified Vulnerability (jul-2011/CVE-2011-0816)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "CMDB Metadata & Instance APIs" 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: 48738

<http://www.securityfocus.com/bid/48738>

\* SECUNIA: 45274

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

**CVE Reference:**

CVE-2011-0816 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 13811 Oracle Database Server - EMCTL component unspecified Vulnerability (jul-2011/CVE-2011-0875)**

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>

\* SECTRACK: 1025795

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

\* BID: 48760

<http://www.securityfocus.com/bid/48760>

\* SECUNIA: 45274

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

**CVE Reference:**

CVE-2011-0875 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 13812 Oracle Database Server - Enterprise Config Management component unspecified Vulnerability (jul-2011/CVE-2011-0831)**

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

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

**References:**

- \* CONFIRM:  
<http://www.oracle.com/technetwork/topics/security/cpuly2011-313328.html>
- \* SECTRACK: 1025795  
<http://www.securitytracker.com/id/1025795>
- \* BID: 48733  
<http://www.securityfocus.com/bid/48733>
- \* SECUNIA: 45274  
<http://secunia.com/advisories/45274/>

**CVE Reference:**

CVE-2011-0831 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13813 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2011/CVE-2011-2230)**

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/cpuly2011-313328.html>
- \* SECTRACK: 1025795  
<http://www.securitytracker.com/id/1025795>
- \* BID: 48743  
<http://www.securityfocus.com/bid/48743>
- \* SECUNIA: 45274  
<http://secunia.com/advisories/45274/>

**CVE Reference:**

CVE-2011-2230 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13814 Oracle Database Server - Enterprise Config Management component unspecified Vulnerability (jul-2011/CVE-2011-0811)**

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

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

**References:**

- \* CONFIRM:  
<http://www.oracle.com/technetwork/topics/security/cpuly2011-313328.html>
- \* SECTRACK: 1025795  
<http://www.securitytracker.com/id/1025795>
- \* BID: 48735  
<http://www.securityfocus.com/bid/48735>
- \* SECUNIA: 45274  
<http://secunia.com/advisories/45274/>

**CVE Reference:**

CVE-2011-0811 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

• **CVE-2011-2399 HP CVSS 2.0 Score = 7.8**

Unspecified vulnerability in the Media Management Daemon (mmd) in HP Data Protector 6.11 and earlier allows remote attackers to cause a denial of service via unknown vectors.

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

**References:**

HP: <http://marc.info/?l=bugtraq&m=131188787531606&w=2>

HP: <http://marc.info/?l=bugtraq&m=131188787531606&w=2>

**CVE Reference:** [CVE-2011-2399](#)

• **CVE-2011-2403 HP CVSS 2.0 Score = 6.5**

SQL injection vulnerability in HP Network Automation 7.2x, 7.5x, 7.6x, 9.0, and 9.10 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors.

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

**References:**

HP: <http://marc.info/?l=bugtraq&m=131188727830971&w=2>

HP: <http://marc.info/?l=bugtraq&m=131188727830971&w=2>

**CVE Reference:** [CVE-2011-2403](#)

• **CVE-2011-2402 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in HP Network Automation 7.2x, 7.5x, 7.6x, 9.0, and 9.10 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

**References:**

HP: <http://marc.info/?l=bugtraq&m=131188727830971&w=2>

HP: <http://marc.info/?l=bugtraq&m=131188727830971&w=2>

**CVE Reference:** [CVE-2011-2402](#)

• **CVE-2011-0252 Apple CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in Apple QuickTime before 7.7 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted STTS atoms in a QuickTime movie file.

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

**References:**

APPLE: <http://lists.apple.com/archives/security-announce/2011/Aug/msg00000.html>

**CVE Reference:** [CVE-2011-0252](#)

• **CVE-2011-0249 Apple CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in Apple QuickTime before 7.7 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted STSC atoms in a QuickTime movie file.

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

**References:**

APPLE: <http://lists.apple.com/archives/security-announce/2011/Aug/msg00000.html>

**CVE Reference:** [CVE-2011-0249](#)

• **CVE-2011-0251 Apple CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in Apple QuickTime before 7.7 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted STSZ atoms in a QuickTime movie file.

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

**References:**

APPLE: <http://lists.apple.com/archives/security-announce/2011/Aug/msg00000.html>

**CVE Reference:** [CVE-2011-0251](#)

• **CVE-2011-0250 Apple CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in Apple QuickTime before 7.7 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted STSS atoms in a QuickTime movie file.

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

**References:**

APPLE: <http://lists.apple.com/archives/security-announce/2011/Aug/msg00000.html>

**CVE Reference:** [CVE-2011-0250](#)

• **CVE-2011-0248 Apple CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in the QuickTime ActiveX control in Apple QuickTime before 7.7 on Windows, when Internet Explorer is used, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted QTL file.

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

**References:**

APPLE: <http://lists.apple.com/archives/security-announce/2011/Aug/msg00000.html>

**CVE Reference:** [CVE-2011-0248](#)

**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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)