

## 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

New type of spam against mobile users. It is hard to know who you can trust. US DOE to analyze power grid cyber threats.

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

### • Spam with QR code targets mobile users

Researchers have revealed a new type of spam campaign that appears to be a test run to find out how mobile users will respond to social engineering attempts on their smartphones and tablets. According to a Tuesday blog post from security firm Websense, the emails look like typical spam trying to hawk male enhancement drugs. However, in this case, they contain a link to a legitimate site -- 2tag.nl -- that generates quick response (QR) codes for URLs.

The link leads to an already-created QR code, which can be scanned by a mobile reader application available in places like the Android Market. After the code is recognized, a URL is loaded that advertises the counterfeit goods, including Viagra and Cialis.

"This is a clear movement and evolution of traditional spammers toward&nbsp;targeting&nbsp;mobile technology," Elad Sharf, a Websense Security Labs researcher, wrote in the blog post. SC Magazine

Full Story :

[http://www.scmagazine.com/spam-with-qr-code-targets-mobile-users/article/222640/?utm\\_source=feedburner&utm](http://www.scmagazine.com/spam-with-qr-code-targets-mobile-users/article/222640/?utm_source=feedburner&utm)

## • **FTC settles with rewards company over security infractions**

A company that helps students save for college may have made them richer, but also could have opened them up to fraud.

The company, Upromise, which is owned by Sallie Mae, failed to live up to its vow to keep customers secure, which violated federal law, the FTC said Thursday in a news release announcing a settlement.

Upromise, which adds small amounts of money to a savings account when users buy items from their partner merchants, asked users to download a "TurboSaver Toolbar" so they could locate merchants that provide rebates. The company encouraged customers to enable the "Personalized Offers" component of the toolbar because, Upromise said, it would allow them to get more customized deals. SC Magazine

Full Story :

[http://www.scmagazine.com/ftc-settles-with-rewards-company-over-security-infractions/article/222391/?utm\\_source=](http://www.scmagazine.com/ftc-settles-with-rewards-company-over-security-infractions/article/222391/?utm_source=)

## • **Energy Department to analyze power grid cyber threats**

U.S. Energy Secretary Steven Chu has unveiled an initiative that seeks to further protect the power grid from cyber attacks. The Electric Sector Cybersecurity Risk Management Maturity project, a federal program to find and contain gaps in the cyber security defenses protecting the nation's electric grid, will be headed by the Department of Energy (DOE), with assistance from the Department of Homeland Security (DHS) and the private sector. The program originated from a proposal from the White House.

"Establishing a comprehensive cyber security approach will give utility companies and grid operators another important tool to improve the grid's ability to respond to cybersecurity risks," Chu said in news release last week.

Patrick Miller, president and CEO of the National Electric Sector Cybersecurity Organization, a nonprofit that supports organizations operating within the energy sector, said the DOE is the right choice to assess how the grid will behave, should there be an attack. SC Magazine

Full Story :

[http://www.scmagazine.com/energy-department-to-analyze-power-grid-cyber-threats/article/222399/?utm\\_source=feed](http://www.scmagazine.com/energy-department-to-analyze-power-grid-cyber-threats/article/222399/?utm_source=feed)

## • **Secret Service charges Romanian man with ATM fraud**

Federal authorities have arrested a Romanian man accused of playing a primary role in an ATM fraud racket.

According to the U.S. attorney's office in New York, Laurentiu Bulat installed electronic skimming devices -- which included card readers and cameras to record personal identification numbers -- on at least 40 ATMs at HSBC bank branches in Manhattan, Long Island and Westchester County, N.Y.

Bulat and his unidentified co-conspirators eventually retrieved the devices, which recorded data that was used to create cloned cards and steal at least \$1.5 million from customer accounts. SC Magazine

Full Story :

[http://www.scmagazine.com/secret-service-charges-romanian-man-with-atm-fraud/article/222301/?utm\\_source=feed](http://www.scmagazine.com/secret-service-charges-romanian-man-with-atm-fraud/article/222301/?utm_source=feed)

# **New Vulnerabilities Tested in SecureScout**

## • **19691 Mozilla Firefox unspecified WebGL test case vulnerability (CVE-2011-3003)**

Mozilla Firefox before 7.0 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unspecified WebGL test case that triggers a memory-allocation error and a resulting out-of-bounds write operation.

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

### **References:**

\* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-41.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=682335](https://bugzilla.mozilla.org/show_bug.cgi?id=682335)

\* MANDRIVA: MDVSA-2011:141

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:141>

### **CVE Reference:**

CVE-2011-3003 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19692 Mozilla Firefox handling XPCNativeWrappers vulnerability (CVE-2011-3004)

The JSSubScriptLoader in Mozilla Firefox 4.x through 6 does not properly handle XPCNativeWrappers during calls to the loadSubScript method in an add-on, which makes it easier for remote attackers to gain privileges via a crafted web site that leverages certain unwrapping behavior.

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

#### References:

\* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-43.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=653926](https://bugzilla.mozilla.org/show_bug.cgi?id=653926)

\* MANDRIVA: MDVSA-2011:141

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:141>

#### CVE Reference:

CVE-2011-3004 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19693 Mozilla Firefox Use-after-free vulnerability (CVE-2011-3005)

Use-after-free vulnerability in Mozilla Firefox 4.x through 6 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OGG headers in a .ogg file.

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

#### References:

\* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-44.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=675747](https://bugzilla.mozilla.org/show_bug.cgi?id=675747)

\* MANDRIVA: MDVSA-2011:141

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:141>

\* MANDRIVA: MDVSA-2011:142

<http://www.mandriva.com/security/advisories?name=MDVSA-2011:142>

\* SUSE: openSUSE-SU-2011:1076

<http://lists.opensuse.org/opensuse-updates/2011-10/msg00002.html>

\* SECUNIA: 46315

<http://secunia.com/advisories/46315>

#### CVE Reference:

CVE-2011-3005 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19694 Mozilla Firefox Integer underflow vulnerability (CVE-2011-2998)

Integer underflow in Mozilla Firefox 3.6.x before 3.6.23 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via JavaScript code containing a large RegExp expression.

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

#### References:

NULL

#### CVE Reference:

CVE-2011-2998 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19722 Mozilla Firefox marquee elements memory corruption vulnerability (CVE-2011-0074)

Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19 and 3.6.x before 3.6.17 allows 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: **Medium**

#### References:

\* CONFIRM:

<http://www.mozilla.org/security/announce/2011/mfsa2011-12.html>

\* CONFIRM:

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=635977](https://bugzilla.mozilla.org/show_bug.cgi?id=635977)

\* DEBIAN: DSA-2227  
<http://www.debian.org/security/2011/dsa-2227>  
\* DEBIAN: DSA-2228  
<http://www.debian.org/security/2011/dsa-2228>  
\* DEBIAN: DSA-2235  
<http://www.debian.org/security/2011/dsa-2235>  
\* MANDRIVA: MDVSA-2011:080  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:080>  
\* MANDRIVA: MDVSA-2011:079  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:079>

#### CVE Reference:

CVE-2011-0075 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19723 Mozilla Firefox privilege escalation vulnerability (CVE-2011-0076)

Unspecified vulnerability in the Java Embedding Plugin (JEP) in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17 allows remote attackers to bypass intended access restrictions via unknown vectors.

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

#### References:

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-15.html>  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=634724](https://bugzilla.mozilla.org/show_bug.cgi?id=634724)  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=644682](https://bugzilla.mozilla.org/show_bug.cgi?id=644682)  
\* MANDRIVA: MDVSA-2011:079  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:079>

#### CVE Reference:

CVE-2011-0076 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19724 Mozilla Firefox double free memory corruption vulnerability (CVE-2011-0070)

Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19, 3.6.x before 3.6.17, and 4.x before 4.0.1 allows 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: **Medium**

#### References:

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-12.html>  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=645565](https://bugzilla.mozilla.org/show_bug.cgi?id=645565)  
\* DEBIAN: DSA-2227  
<http://www.debian.org/security/2011/dsa-2227>  
\* DEBIAN: DSA-2228  
<http://www.debian.org/security/2011/dsa-2228>  
\* DEBIAN: DSA-2235  
<http://www.debian.org/security/2011/dsa-2235>  
\* MANDRIVA: MDVSA-2011:080  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:080>  
\* MANDRIVA: MDVSA-2011:079  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:079>

#### CVE Reference:

CVE-2011-0070 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19725 Mozilla Firefox information disclosure vulnerability (CVE-2011-0067)

Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17 does not properly implement autocompletion for forms, which allows remote attackers to read form history entries via a Java applet that spoofs interaction with the autocomplete controls.

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

#### References:

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-12.html>  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=644069](https://bugzilla.mozilla.org/show_bug.cgi?id=644069)  
\* DEBIAN: DSA-2227  
<http://www.debian.org/security/2011/dsa-2227>  
\* DEBIAN: DSA-2228  
<http://www.debian.org/security/2011/dsa-2228>  
\* DEBIAN: DSA-2235  
<http://www.debian.org/security/2011/dsa-2235>  
\* MANDRIVA: MDVSA-2011:080  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:080>  
\* MANDRIVA: MDVSA-2011:079  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:079>

#### CVE Reference:

CVE-2011-0069 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19726 Mozilla Firefox OBJECT 'mObserverList' Use-After-Free vulnerability (CVE-2011-0066)

Use-after-free vulnerability in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17 allows remote attackers to execute arbitrary code via vectors related to OBJECT's mObserverList.

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

#### References:

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-13.html>  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=634983](https://bugzilla.mozilla.org/show_bug.cgi?id=634983)  
\* DEBIAN: DSA-2227  
<http://www.debian.org/security/2011/dsa-2227>  
\* DEBIAN: DSA-2228  
<http://www.debian.org/security/2011/dsa-2228>  
\* DEBIAN: DSA-2235  
<http://www.debian.org/security/2011/dsa-2235>  
\* MANDRIVA: MDVSA-2011:079  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:079>

#### CVE Reference:

CVE-2011-0066 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19727 Mozilla Firefox cross-domain javascript memory corruption vulnerability (CVE-2011-0069)

Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19, 3.6.x before 3.6.17, and 4.x before 4.0.1 allows 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: **Medium**

#### References:

\* CONFIRM:  
<http://www.mozilla.org/security/announce/2011/mfsa2011-12.html>  
\* CONFIRM:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=644069](https://bugzilla.mozilla.org/show_bug.cgi?id=644069)  
\* DEBIAN: DSA-2227  
<http://www.debian.org/security/2011/dsa-2227>  
\* DEBIAN: DSA-2228  
<http://www.debian.org/security/2011/dsa-2228>  
\* DEBIAN: DSA-2235  
<http://www.debian.org/security/2011/dsa-2235>  
\* MANDRIVA: MDVSA-2011:080  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:080>  
\* MANDRIVA: MDVSA-2011:079  
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:079>

#### CVE Reference:

CVE-2011-0069 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

# New Vulnerabilities found this Week

## • CVE-2012-0013 Microsoft CVSS 2.0 Score = 9.3

Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability."

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

### References:

MS: <http://technet.microsoft.com/security/bulletin/MS12-005>

CVE Reference: [CVE-2012-0013](#)

## • CVE-2012-0004 Microsoft CVSS 2.0 Score = 9.3

Unspecified vulnerability in DirectShow in DirectX in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted media file, related to Quartz.dll, Qdvd.dll, and the Line21 DirectShow filter, aka "DirectShow Remote Code Execution Vulnerability."

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

### References:

MS: <http://technet.microsoft.com/security/bulletin/MS12-004>

CVE Reference: [CVE-2012-0004](#)

## • CVE-2012-0001 Microsoft CVSS 2.0 Score = 9.3

The kernel in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly load structured exception handling tables, which allows context-dependent attackers to bypass the SafeSEH security feature by leveraging a Visual C++ .NET 2003 application, aka "Windows Kernel SafeSEH Bypass Vulnerability."

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

### References:

MS: <http://technet.microsoft.com/security/bulletin/MS12-001>

CVE Reference: [CVE-2012-0001](#)

## • CVE-2012-0003 Microsoft CVSS 2.0 Score = 9.3

Unspecified vulnerability in winmm.dll in Windows Multimedia Library in Windows Media Player (WMP) in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted MIDI file, aka "MIDI Remote Code Execution Vulnerability."

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

### References:

MS: <http://technet.microsoft.com/security/bulletin/MS12-004>

CVE Reference: [CVE-2012-0003](#)

## • CVE-2012-0005 Microsoft CVSS 2.0 Score = 6.9

The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2, when a Chinese, Japanese, or Korean system locale is used, can access uninitialized memory during the processing of Unicode characters, which allows local users to gain privileges via a crafted application, aka "CSRSS Elevation of Privilege Vulnerability."

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

### References:

MS: <http://technet.microsoft.com/security/bulletin/MS12-003>

CVE Reference: [CVE-2012-0005](#)

• **CVE-2012-0009 Microsoft CVSS 2.0 Score = 4.4**

Untrusted search path vulnerability in the Windows Object Packager configuration in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a Trojan horse executable file in the current working directory, as demonstrated by a directory that contains a file with an embedded packaged object, aka "Object Packager Insecure Executable Launching Vulnerability."

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

**References:**

MS: <http://technet.microsoft.com/security/bulletin/MS12-002>

**CVE Reference:** [CVE-2012-0009](#)

• **CVE-2012-0392 Apache CVSS 2.0 Score = 9.3**

The CookieInterceptor component in Apache Struts before 2.3.1.1 does not use the parameter-name whitelist, which allows remote attackers to execute arbitrary commands via a crafted HTTP Cookie header that triggers Java code execution through a static method.

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

**References:**

MISC: [https://www.sec-consult.com/files/20120104-0\\_Apache\\_Struts2\\_Multiple\\_Critical\\_Vulnerabilities.txt](https://www.sec-consult.com/files/20120104-0_Apache_Struts2_Multiple_Critical_Vulnerabilities.txt)

MLIST: <https://lists.immunityinc.com/pipermail/dailydave/2012-January/000011.html>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/18329>

CONFIRM: <http://struts.apache.org/2.x/docs/version-notes-2311.html>

CONFIRM: <http://struts.apache.org/2.x/docs/s2-008.html>

SECUNIA: <http://secunia.com/advisories/47393>

BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2012-01/0031.html>

**CVE Reference:** [CVE-2012-0392](#)

• **CVE-2012-0391 Apache CVSS 2.0 Score = 9.3**

The ExceptionDelegator component in Apache Struts before 2.2.3.1 interprets parameter values as OGNL expressions during certain exception handling for mismatched data types of properties, which allows remote attackers to execute arbitrary Java code via a crafted parameter.

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

**References:**

MISC: [https://www.sec-consult.com/files/20120104-0\\_Apache\\_Struts2\\_Multiple\\_Critical\\_Vulnerabilities.txt](https://www.sec-consult.com/files/20120104-0_Apache_Struts2_Multiple_Critical_Vulnerabilities.txt)

CONFIRM: <https://issues.apache.org/jira/browse/WW-3668>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/18329>

CONFIRM: <http://struts.apache.org/2.x/docs/version-notes-2311.html>

CONFIRM: <http://struts.apache.org/2.x/docs/s2-008.html>

SECUNIA: <http://secunia.com/advisories/47393>

BUGTRAQ: <http://archives.neohapsis.com/archives/bugtraq/2012-01/0031.html>

**CVE Reference:** [CVE-2012-0391](#)

**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)