

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

Arrests in Anonymous investigation. NATO still under attack from Anonymous. Microsoft offers reward for finding Rustock mastermind. Anonymous claim to have sensitive NATO information.

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

• FBI arrests more than a dozen in Anonymous hacking investigation

Sixteen people were arrested in the United States today in connection with hacking attacks by the Anonymous group of online activists, as well as one person in the U.K. and four people in the Netherlands, the U.S. Department of Justice said.

An indictment filed last week in San Jose, Calif., names 14 people accused of conspiring to intentionally damage protected computers at PayPal last December in retribution for PayPal dropping support for monetary donations made to WikiLeaks. The arrests were made in Alabama, Arizona, California, Colorado, the District of Columbia, Florida, Massachusetts, Nevada, New Mexico, and Ohio, the DOJ said.

In two other separate cases, a man was arrested in Florida on charges of accessing the Web site of InfraGard Tampa Bay, an FBI partner, in June, and a man was arrested in Las Cruces, N.M., for allegedly stealing confidential business information from AT&T servers and posting it publicly in June, according to indictments. Cnet Security

Full Story :

• **Anonymous still accessing, downloading NATO data**

The North Atlantic Treaty Organization is still under attack, a person claiming to be a member of Anonymous told CBS News in an interview published today.

According to the alleged member, who uses the name "Commander X," the "hactivist" group still has access to NATO servers and is currently "downloading databases." What's more, the person said that the group plans to release all the documents it has collected, even though a Twitter account related to the organization says such a release would be "irresponsible."

"Anonymous ALWAYS releases EVERYTHING we take...eventually," Commander X wrote in an e-mail to CBS News, which is owned by CBS, the same company that owns CNET. "But with these big classified dumps we like to take our time analyzing exactly what it is we have. That way we can do the disclosures in such a way as to maximize the political impact of the release." Cnet Security

Full Story :

http://news.cnet.com/8301-13506_3-20081890-17/anonymous-still-accessing-downloading-nato-data/?part=rss&sub

• **Microsoft offers \$250K reward to find Rustock masterminds**

Fresh off releasing new stats showing that more than half of machines once infected with the Rustock trojan have been cleaned, Microsoft is turning its attention to finding the masterminds responsible for the botnet.

The software giant is offering a \$250,000 reward for information that leads to the arrest and conviction of the Rustock operators, Microsoft senior attorney Richard Boscovich announced Monday in a blog post.

The move follows a Microsoft-led takedown operation in March, which involved cutting off command-and-control centers from being able to communicate with Rustock-infected machines and filing a lawsuit against 11 unnamed defendants. SC Magazine

Full Story :

http://www.scmagazineus.com/microsoft-offers-250k-reward-to-find-rustock-masterminds/article/207765/?utm_source

• **Anonymous, LulzSec flex muscles after FBI takedowns**

Hactivist group Anonymous said Thursday that it is sitting on a large amount of sensitive information belonging to the North American Treaty Organization (NATO).

The collective said on Twitter that it siphoned about 1 gigabyte (GB) of data from the servers of NATO, but said it would be "irresponsible" to publish the trove. The group used an injection-style attack in order to gain access, according to another tweet.

A NATO spokesperson could not be reached, but according to published reports, a representative condemned the attacks and said the organization is investigating. SC Magazine

Full Story :

http://www.scmagazineus.com/anonymous-lulzsec-flex-muscles-after-fbi-takedowns/article/208085/?utm_source=feed

• **Breach law passes hurdle, but faces opposition**

A House of Representatives subcommittee on Wednesday approved legislation that would establish a national data breach notification law and require companies to implement data protection policies.

But it appears the measure faces an uphill climb, similar to past data breach notification proposals that never were enacted into law.

Following a lengthy debate, the bill, Secure and Fortify Electronic (SAFE) Data Act, passed the House Subcommittee on Commerce, Manufacturing and Trade. Introduced by Rep. Mary Bono Mack, R-Calif., the legislation would pre-empt state data breach notification laws and require compromised companies to notify the Federal Trade Commission and affected individuals within 48 hours of determining those whose personal information was lost or stolen. SC Magazine

Full Story :

http://www.scmagazineus.com/breach-law-passes-hurdle-but-faces-opposition/article/208067/?utm_source=feed

New Vulnerabilities Tested in SecureScout

• 19401 Adobe Acrobat / Reader security bypass Vulnerability (CVE-2011-2102) (Remote File Checking)

Unspecified vulnerability in Adobe Reader and Acrobat before 10.1 on Windows and Mac OS X allows attackers to bypass intended access restrictions via unknown vectors.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
- * BID: 48253
<http://www.securityfocus.com/bid/48253>
- * SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2102 (cve.mitre.org, nvd.nist.gov)

• 19402 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2011-2103) (Remote File Checking)

Adobe Reader and Acrobat 8.x before 8.3 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
- * BID: 48247
<http://www.securityfocus.com/bid/48247>
- * SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2103 (cve.mitre.org, nvd.nist.gov)

• 19403 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2011-2104) (Remote File Checking)

Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to cause a denial of service (memory corruption) via unspecified vectors.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
- * BID: 48251
<http://www.securityfocus.com/bid/48251>
- * SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2104 (cve.mitre.org, nvd.nist.gov)

• 19404 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2011-2105) (Remote File Checking)

Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.

Adobe recommends users of Adobe Reader X (10.x) and earlier versions for Windows and Macintosh to update to Adobe Reader X (10.1). For users of Adobe Reader 9.4.4 and earlier versions for Windows and Macintosh, who cannot update to Adobe Reader X (10.1), Adobe has made available updates, Adobe Reader 9.4.5 and Adobe Reader 8.3. Adobe recommends users of Adobe Acrobat X (10.0.3) for Windows and Macintosh update to Adobe Acrobat X (10.1). Adobe recommends users of Adobe Acrobat 9.4.4 and earlier versions for Windows and Macintosh update to Adobe Acrobat 9.4.5, and users of Adobe Acrobat 8.2.6 and earlier versions for Windows and Macintosh update to Adobe Acrobat 8.3.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-16.html>
- * BID: 48248
<http://www.securityfocus.com/bid/48248>
- * SECTRACK: 1025658
<http://securitytracker.com/id/1025658>

CVE Reference:

CVE-2011-2105 (cve.mitre.org, nvd.nist.gov)

• 19415 Win32k Use After Free Vulnerability (CVE-2011-1884) (MS11-054/2555917) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48596
<http://www.securityfocus.com/bid/48596>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1884 (cve.mitre.org, nvd.nist.gov)

• 19416 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1885) (MS11-054/2555917) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48600
<http://www.securityfocus.com/bid/48600>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1885 (cve.mitre.org, nvd.nist.gov)

• 19417 Win32k Incorrect Parameter Allows Information Disclosure Vulnerability (CVE-2011-1886) (MS11-054/2555917) (Remote File Checking)

An information disclosure vulnerability exists due to the way that Windows kernel-mode drivers validate function parameters. An attacker who successfully exploited this vulnerability could access data from any kernel-mode memory location, including access to the SAM file.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48607
<http://www.securityfocus.com/bid/48607>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1886 (cve.mitre.org, nvd.nist.gov)

• 19418 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1887) (MS11-054/2555917) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48601
<http://www.securityfocus.com/bid/48601>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1887 (cve.mitre.org, nvd.nist.gov)

• 19419 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1888) (MS11-054/2555917) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48603
<http://www.securityfocus.com/bid/48603>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1888 (cve.mitre.org, nvd.nist.gov)

• 19420 Microsoft Visio Insecure Library Loading Vulnerability (MS11-055/2560847) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Visio handles the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* EXPLOIT-DB: 14744

<http://www.exploit-db.com/exploits/14744/>

* MS: MS11-055

<http://www.microsoft.com/technet/security/Bulletin/MS11-055.msp>

* OVAL: oval:org.mitre.oval:def:7122

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7122>

* VUPEN: ADV-2010-2192

<http://www.vupen.com/english/advisories/2010/2192>

CVE Reference:

CVE-2010-3148 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-2288 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in Sun Integrated Lights Out Manager (ILOM) in SysFW 8.1.0.a and earlier for various Oracle SPARC T3, SPARC Netra T3, Sun Blade, and Sun Fire servers allows remote attackers to affect confidentiality, integrity, and availability, related to ILOM.

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

References:

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

CVE Reference: [CVE-2011-2288](#)**• CVE-2011-2261 Oracle CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.3.0.3 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

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

CVE Reference: [CVE-2011-2261](#)**• CVE-2011-2307 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in Oracle SysFW 8.1.0.a in various Oracle SPARC T3, Netra SPARC T3, Sun Fire, and Sun Blade servers allows remote attackers to affect confidentiality, integrity, and availability, related to Sun Integrated Lights Out Manager (ILOM). Per: <http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>
'CVE-2011-2307: Specific products affected are: SPARC T3-1, SPARC T3-1B, SPARC T3-2, SPARC T3-4, Netra SPARC T3-1, Netra SPARC T3-1B, Sun Fire X4170 M2, Sun Fire X4270 M2, Sun Blade x6270 M2, Sun Fire x4470, Sun Fire x4470 M2'

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

References:

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

CVE Reference: [CVE-2011-2307](#)

• **CVE-2011-2299 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in Oracle SPARC Enterprise M3000, M4000, M5000, M8000, and M9000 XCP 1101 and earlier allows remote attackers to affect confidentiality, integrity, and availability, related to XSCF Control Package (XCP).

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

References:

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

CVE Reference: [CVE-2011-2299](#)

• **CVE-2011-2245 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the Solaris component in Oracle Sun Products Suite 9 and 10 allows remote attackers to affect confidentiality, integrity, and availability, related to SSH.

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

References:

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

CVE Reference: [CVE-2011-2245](#)

• **CVE-2011-2239 Oracle CVSS 2.0 Score = 7.1**

Unspecified vulnerability in the Core RDBMS component in Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, and 11.2.0.2 allows remote authenticated users to affect confidentiality, integrity, and availability, related to XMLSEQ_IMP_T.

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

References:

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

CVE Reference: [CVE-2011-2239](#)

• **CVE-2011-2253 Oracle CVSS 2.0 Score = 7.1**

Unspecified vulnerability in the Core RDBMS component in Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, and 11.2.0.2 allows remote authenticated users to affect confidentiality, integrity, and availability, related to SYSDBA.

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

References:

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

CVE Reference: [CVE-2011-2253](#)

• **CVE-2011-2257 Oracle CVSS 2.0 Score = 6.8**

Unspecified vulnerability in the Database Target Type Menu component in Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, and 11.2.0.2; and Oracle Enterprise Manager Grid Control 10.1.0.6, 10.2.0.5, and 11.1.0.1; allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

References:

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

CVE Reference: [CVE-2011-2257](#)

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