

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://www.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

Does data breach notification carry risk of ID theft? Web sites just keep getting more and more infected. Avalanche the most active phishing group. Smart grid roll-out with stimulus funds.

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

• Data breach alerts linked to increased risk of ID theft

Consumers who have received a data breach notification letter are four times more likely than others to be the victim of identity theft, according to a survey released this week by Javelin Strategy and Research.

Approximately 11 percent of U.S. consumers have received a data breach notification letter in the past 12 months with a third of the breaches involving Social Security numbers and 15 percent involving ATM PINs, according to Javelin's third annual survey of nearly 5,000 U.S. consumers, released Tuesday.

Of those who have received a data breach notification letter in the past year, 19.5 percent said they were the victims of fraud associated with identity theft, compared to 4.3 percent who have not received a notification but were victimized.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Data-breach-alerts-linked-to-increased-risk-of-ID-theft/article/156376/>

• **New data shows website hacks continue to grow unabated**

More than two million more web pages were infected with malware during the third quarter of 2009 compared to the same quarter last year, according to data gathered by web anti-malware vendor Dasient.

From July until September, approximately 640,000 different websites - and a total of 5.8 million pages on those sites - were infected to distribute malware, Dasient found through studying data collected on its malware analysis platform.

Those numbers represent a noticeable spike compared to data published by Microsoft in April that found approximately three million web pages were infected with malware during the third quarter of 2008, Ameet Ranadive, co-founder of Dasient, told SCMagazineUS.com on Tuesday. SC Magazine

Full Story :

<http://www.scmagazineus.com/New-data-shows-website-hacks-continue-to-grow-unabated/article/156291/>

• **Avalanche the most prolific phishing group of 2009**

A criminal phishing group called Avalanche was responsible for nearly a quarter of all phishing attacks identified during the first half of this year, according to a recently released Anti-Phishing Working Group (APWG) report.

"Avalanche began attacks in December 2008 and ramped up significantly in early 2009, quickly becoming the most prolific and dangerous operation on the internet," the report states.

The Avalanche cybercrime group, which has spoofed more than 30 financial institutions, along with other online services and job search companies, was responsible for 24 percent of all phishing attacks during the first half of the year, according to the APWG's Global Phishing Survey, released last week. SC Magazine

Full Story :

<http://www.scmagazineus.com/Avalanche-the-most-prolific-phishing-group-of-2009/article/156216/>

• **Smart grid gets multibillion-dollar injection**

The U.S. electricity grid will get a 21st century upgrade, including installation of millions of smart meters, through a government-led program.

The Obama administration is scheduled to announce Tuesday where it is spending \$3.4 billion of stimulus money on 100 smart-grid projects in 49 states. As part of the funding, utilities are contributing \$4.7 billion to the projects, making the total spending \$8.1 billion.

Images: The many faces of the smart grid View the full gallery Cnet Security

Full Story :

http://news.cnet.com/8301-11128_3-10383729-54.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• **18578 GDI+ WMF Integer Overflow Vulnerability (MS09-062/957488) (Remote File Checking)**

A remote code execution vulnerability exists in the way that GDI+ allocates buffer size when handling WMF image files. The vulnerability could allow remote code execution if a user opens a specially crafted WMF image file or browses to a Web site that contains specially crafted content. 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:

* MS: MS09-062

<http://www.microsoft.com/technet/security/Bulletin/MS09-062.msp>

* BID: 36619

<http://www.securityfocus.com/bid/36619>

* VUPEN: VUPEN/ADV-2009-2897

<http://www.vupen.com/english/advisories/2009/2897>

* SECTRACK: 1023006

<http://securitytracker.com/alerts/2009/Oct/1023006.html>

CVE Reference:

CVE-2009-2500 (cve.mitre.org, nvd.nist.gov)

• 18579 GDI+ PNG Heap Overflow Vulnerability (MS09-062/957488) (Remote File Checking)

A remote code execution vulnerability exists in the way that GDI+ allocates memory. The vulnerability could allow remote code execution if a user opens a specially crafted PNG image file. 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:

- * MS: MS09-062
<http://www.microsoft.com/technet/security/Bulletin/MS09-062.msp>
- * BID: 36645
<http://www.securityfocus.com/bid/36645>
- * VUPEN: VUPEN/ADV-2009-2897
<http://www.vupen.com/english/advisories/2009/2897>
- * SECTRACK: 1023006
<http://securitytracker.com/alerts/2009/Oct/1023006.html>

CVE Reference:

CVE-2009-2501 (cve.mitre.org, nvd.nist.gov)

• 18580 GDI+ TIFF Buffer Overflow Vulnerability (MS09-062/957488) (Remote File Checking)

A remote code execution vulnerability exists in the way that GDI+ allocates memory. The vulnerability could allow remote code execution if a user opens a specially crafted TIFF file. 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:

- * MS: MS09-062
<http://www.microsoft.com/technet/security/Bulletin/MS09-062.msp>
- * BID: 36646
<http://www.securityfocus.com/bid/36646>
- * VUPEN: VUPEN/ADV-2009-2897
<http://www.vupen.com/english/advisories/2009/2897>
- * SECTRACK: 1023006
<http://securitytracker.com/alerts/2009/Oct/1023006.html>

CVE Reference:

CVE-2009-2502 (cve.mitre.org, nvd.nist.gov)

• 18581 GDI+ TIFF Memory Corruption Vulnerability (MS09-062/957488) (Remote File Checking)

A remote code execution vulnerability exists in the way that GDI+ allocates memory. The vulnerability could allow remote code execution if a user opens a specially crafted TIFF file. 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:

- * MS: MS09-062
<http://www.microsoft.com/technet/security/Bulletin/MS09-062.msp>
- * BID: 36647
<http://www.securityfocus.com/bid/36647>
- * VUPEN: VUPEN/ADV-2009-2897
<http://www.vupen.com/english/advisories/2009/2897>
- * SECTRACK: 1023006
<http://securitytracker.com/alerts/2009/Oct/1023006.html>

CVE Reference:

CVE-2009-2503 (cve.mitre.org, nvd.nist.gov)

• 18582 GDI+ .NET API Vulnerability (MS09-062/957488) (Remote File Checking)

A remote code execution vulnerability exists in GDI+ that can allow a malicious Microsoft .NET application to gain unmanaged code execution privileges.. Microsoft .NET applications that are not malicious are not at risk for being compromised because of this vulnerability.

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

References:

- * MS: MS09-062
<http://www.microsoft.com/technet/security/Bulletin/MS09-062.msp>
- * BID: 36648
<http://www.securityfocus.com/bid/36648>
- * VUPEN: VUPEN/ADV-2009-2897
<http://www.vupen.com/english/advisories/2009/2897>
- * SECTRACK: 1023006
<http://securitytracker.com/alerts/2009/Oct/1023006.html>

CVE Reference:

CVE-2009-2504 (cve.mitre.org, nvd.nist.gov)

• 18583 GDI+ PNG Integer Overflow Vulnerability (MS09-062/957488) (Remote File Checking)

A remote code execution vulnerability exists in the way that GDI+ allocates memory. The vulnerability could allow remote code execution if a user opens a specially crafted PNG image file. 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:

- * MS: MS09-062
<http://www.microsoft.com/technet/security/Bulletin/MS09-062.msp>
- * BID: 36649
<http://www.securityfocus.com/bid/36649>
- * VUPEN: VUPEN/ADV-2009-2897
<http://www.vupen.com/english/advisories/2009/2897>
- * SECTRACK: 1023006
<http://securitytracker.com/alerts/2009/Oct/1023006.html>

CVE Reference:

CVE-2009-3126 (cve.mitre.org, nvd.nist.gov)

• 18584 Memory Corruption Vulnerability (MS09-062/957488) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file that includes a malformed object. 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.

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

References:

- * MS: MS09-062
<http://www.microsoft.com/technet/security/Bulletin/MS09-062.msp>
- * BID: 36650
<http://www.securityfocus.com/bid/36650>
- * VUPEN: VUPEN/ADV-2009-2897
<http://www.vupen.com/english/advisories/2009/2897>
- * SECTRACK: 1023006
<http://securitytracker.com/alerts/2009/Oct/1023006.html>

CVE Reference:

CVE-2009-2528 (cve.mitre.org, nvd.nist.gov)

• 18585 Office BMP Integer Overflow Vulnerability (MS09-062/957488) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office handles specially crafted Office Documents containing BMP images. The vulnerability could allow remote code execution if an Outlook user opens a

specially crafted e-mail or opens an Office Document with a malformed Bitmap file. 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:

- * MS: MS09-062
<http://www.microsoft.com/technet/security/Bulletin/MS09-062.msp>
- * BID: 36651
<http://www.securityfocus.com/bid/36651>
- * VUPEN: VUPEN/ADV-2009-2897
<http://www.vupen.com/english/advisories/2009/2897>
- * SECTRACK: 1023006
<http://securitytracker.com/alerts/2009/Oct/1023006.html>

CVE Reference:

CVE-2009-2518 (cve.mitre.org, nvd.nist.gov)

• 18586 Memory Corruption in Indexing Service Vulnerability (MS09-057/969059) (Remote File Checking)

A remote code execution vulnerability exists in the Indexing Service on Windows systems. The vulnerability is due to an ActiveX control included with the service not properly handling specifically crafted Web content. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

- * BID: 36629
<http://www.securityfocus.com/bid/36629>
- * VUPEN: VUPEN/ADV-2009-2892
<http://www.vupen.com/english/advisories/2009/2892>
- * SECTRACK: 1023011
<http://securitytracker.com/alerts/2009/Oct/1023011.html>
- * MS: MS09-057
<http://www.microsoft.com/technet/security/Bulletin/MS09-057.msp>

CVE Reference:

CVE-2009-2507 (cve.mitre.org, nvd.nist.gov)

• 18587 Local Security Authority Subsystem Service Integer Overflow Vulnerability (MS09-059/975467) (Remote File Checking)

A denial of service vulnerability exists in the Microsoft Windows Local Security Authority Subsystem Service (LSASS) due to its improper handling of malformed packets during NTLM authentication. An attacker could create specially crafted anonymous NTLM authentication requests that would cause the LSASS service to stop responding and subsequently restart the computer.

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

References:

- * BID: 36593
<http://www.securityfocus.com/bid/36593>
- * VUPEN: VUPEN/ADV-2009-2894
<http://www.vupen.com/english/advisories/2009/2894>
- * SECTRACK: 1023010
<http://securitytracker.com/alerts/2009/Oct/1023010.html>
- * MS: MS09-059
<http://www.microsoft.com/technet/security/Bulletin/MS09-059.msp>

CVE Reference:

CVE-2009-2524 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- CVE-2009-3821 Apache CVSS 2.0 Score = 4.3

Cross-site scripting (XSS) vulnerability in the Apache Solr Search (solr) extension 1.0.0 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

CONFIRM: <http://typo3.org/teams/security/security-bulletins/typo3-sa-2009-014/>

CVE Reference: [CVE-2009-3821](#)

• **CVE-2009-3816 IBM CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in Activities pages in the Mobile subsystem in IBM Lotus Connections 2.5.0.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg24024303>

SECUNIA: <http://secunia.com/advisories/37106>

CVE Reference: [CVE-2009-3816](#)

• **CVE-2009-1563 Mozilla CVSS 2.0 Score = 10.0**

Array index error in Mozilla Firefox 3.0.x before 3.0.15 and 3.5.x before 3.5.4 allows remote attackers to execute arbitrary code via a long string that triggers incorrect memory allocation and a heap-based buffer overflow during conversion to a floating-point number.

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

References:

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-59.html>

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=516862

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=516396

MISC: http://secunia.com/secunia_research/2009-35/

CVE Reference: [CVE-2009-1563](#)

• **CVE-2009-3371 Mozilla CVSS 2.0 Score = 10.0**

Use-after-free vulnerability in Mozilla Firefox 3.5.x before 3.5.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by creating JavaScript web-workers recursively.

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

References:

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-54.html>

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=514554

CVE Reference: [CVE-2009-3371](#)

• **CVE-2009-3372 Mozilla CVSS 2.0 Score = 9.3**

Mozilla Firefox before 3.0.15 and 3.5.x before 3.5.4, and SeaMonkey before 2.0, allows remote attackers to execute arbitrary code via a crafted regular expression in a Proxy Auto-configuration (PAC) file.

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

References:

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-55.html>

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=500644

CVE Reference: [CVE-2009-3372](#)

• **CVE-2009-3370 Mozilla CVSS 2.0 Score = 5.0**

Mozilla Firefox before 3.0.15, and 3.5.x before 3.5.4, allows remote attackers to read form history by forging mouse and keyboard events that leverage the auto-fill feature to populate form fields, in an attacker-readable form, with history entries.

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

References:

CONFIRM: https://bugzilla.mozilla.org/show_bug.cgi?id=511615

CONFIRM: <http://www.mozilla.org/security/announce/2009/mfsa2009-52.html>

CVE Reference: [CVE-2009-3370](https://cve.mitre.org/cve/2009/3370)

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