

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

Hard for FED to reach goals. \$12 million for failing to protect customers. Whitepages.com stops ads with malware. Zeus botnet taken offline but not for long.

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

• Report: Federal cybersecurity plan facing barriers

The federal government is facing a number of challenges in its efforts to meet objectives set forth in the recently partially declassified Comprehensive National Cybersecurity Initiative (CNCI), according to a report released on Friday from the Government Accountability Office (GAO).

The GAO was asked by Congress to determine what actions have been taken to plan CNCI activities and what challenges the government faces in achieving the initiative's objectives. The CNCI, a program that began in 2008 under the Bush administration to help secure the United States in cyberspace, consists of 12 projects aimed at reducing vulnerabilities, protecting against intrusions, and anticipating future threats against federal executive branch information systems. SC Magazine

Full Story :

http://www.scmagazineus.com/report-federal-cybersecurity-plan-facing-barriers/article/165383/?utm_source=feedbu

• LifeLock to pay \$12 million to settle deceptive-practices claim

LifeLock CEO Todd Davis

(Credit: LifeLock)

LifeLock has agreed to pay \$12 million to settle charges that the company failed to protect customers against identity fraud as advertised and put customer data at risk. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10466741-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• **WhitePages.com halts ad networks over malware**

(Credit: WhitePages.com)

WhitePages.com has stopped ad networks from delivering ads to its site after they were found to contain fake antivirus malware.

"On Monday morning WhitePages received reports from users [about] malware in the form of a fake antivirus upsell program that we believe originated (against our terms) from a third-party advertising network serving ads on our website, in addition to other websites," a WhitePages spokeswoman said in an e-mail late Tuesday. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10466753-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• **Troyak shutdown signals short-lived win against Zeus**

The takedown of a rogue internet service provider known as "AS Troyak," which was linked to the prolific Zeus botnet, caused a massive, albeit brief, drop in the number of active Zeus command-and-control (C&C) servers this week before attackers reconnected their criminal operations. Troyak, believed to be based in Eastern Europe, is the upstream provider for the top six Zeus-hosting ISPs, according to Zeus Tracker, a website that tracks the botnet. Early Tuesday morning, Troyak was suddenly taken offline, causing a large number of Zeus C&C servers to also lose connectivity. With their internet connection shut off, attackers could not send instructions to compromised machines or receive stolen information from them.

There are many botnets of computers infected with the notorious data-stealing trojan Zeus, known for stealing bank account information from its victims. One recently discovered Zeus botnet was made up of infected computer systems at nearly 2,500 organizations and government agencies worldwide. SC Magazine

Full Story :

http://www.scmagazineus.com/troyak-shutdown-signals-short-lived-win-against-zeus/article/165533/?utm_source=fe

New Vulnerabilities Tested in SecureScout

• **14550 Adobe Acrobat / Reader Mozilla plug-in in remote exploitation Vulnerability (CVE-2009-2991) (Remote File Checking)**

Unspecified vulnerability in the Mozilla plug-in in Adobe Reader and Acrobat 8.x before 8.1.7, and possibly 7.x before 7.1.4 and 9.x before 9.2, might allow remote attackers to execute arbitrary code via unknown vectors.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-15.html>

* CERT: TA09-286B

<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>

* BID: 36638

<http://www.securityfocus.com/bid/36638>

* SECTRACK: 1023007

<http://securitytracker.com/id?1023007>

* VUPEN: ADV-2009-2898

<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2991 (cve.mitre.org, nvd.nist.gov)

• **14551 Adobe Acrobat / Reader input validation issue specific to the ActiveX control Denial of Service Vulnerability (CVE-2009-2992) (Remote File Checking)**

An unspecified ActiveX control in Adobe Reader and Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 does not properly validate input, which allows attackers to cause a denial of service via unknown vectors.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2992 (cve.mitre.org, nvd.nist.gov)

• 14552 Adobe Acrobat / Reader multiple input validation Vulnerabilities (CVE-2009-2993) (Remote File Checking)

The JavaScript for Acrobat API in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 does not properly implement the (1) Privileged Context and (2) Safe Path restrictions for unspecified JavaScript methods, which allows remote attackers to create arbitrary files, and possibly execute arbitrary code, via the cPath parameter in a crafted PDF file. NOTE: some of these details are obtained from third party information.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- * CERT: TA09-286B
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- * CERT-VN: VU#257117
<http://www.kb.cert.org/vuls/id/257117>
- * BID: 36638
<http://www.securityfocus.com/bid/36638>
- * BID: 36664
<http://www.securityfocus.com/bid/36664>
- * SECTRACK: 1023007
<http://securitytracker.com/id?1023007>
- * VUPEN: ADV-2009-2898
<http://www.vupen.com/english/advisories/2009/2898>

CVE Reference:

CVE-2009-2993 (cve.mitre.org, nvd.nist.gov)

• 18722 Microsoft Office Excel Record Memory Corruption Vulnerability (MS10-017/980150) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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.

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

References:

- * BID: 38547
<http://www.securityfocus.com/bid/38547>
- * VUPEN: VUPEN/ADV-2010-0566
<http://www.vupen.com/english/advisories/2010/0566>
- * SECTRACK: 1023698
<http://securitytracker.com/alerts/2010/Mar/1023698.html>
- * MS: MS10-017
<http://www.microsoft.com/technet/security/bulletin/ms10-017.msp>

CVE Reference:

CVE-2010-0257 (cve.mitre.org, nvd.nist.gov)

• **18723 Microsoft Office Excel Sheet Object Type Confusion Vulnerability (MS10-017/980150) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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.

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

References:

- * BID: 38550
<http://www.securityfocus.com/bid/38550>
- * VUPEN: VUPEN/ADV-2010-0566
<http://www.vupen.com/english/advisories/2010/0566>
- * SECTRACK: 1023698
<http://securitytracker.com/alerts/2010/Mar/1023698.html>
- * MS: MS10-017
<http://www.microsoft.com/technet/security/bulletin/ms10-017.msp>

CVE Reference:

CVE-2010-0258 (cve.mitre.org, nvd.nist.gov)

• **18724 Microsoft Office Excel MDXTUPLE Record Heap Overflow Vulnerability (MS10-017/980150) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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.

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

References:

- * BID: 38551
<http://www.securityfocus.com/bid/38551>
- * VUPEN: VUPEN/ADV-2010-0566
<http://www.vupen.com/english/advisories/2010/0566>
- * SECTRACK: 1023698
<http://securitytracker.com/alerts/2010/Mar/1023698.html>
- * MS: MS10-017
<http://www.microsoft.com/technet/security/bulletin/ms10-017.msp>

CVE Reference:

CVE-2010-0260 (cve.mitre.org, nvd.nist.gov)

• **18725 Microsoft Office Excel MDXSET Record Heap Overflow Vulnerability (MS10-017/980150) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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.

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

References:

- * BID: 38552
<http://www.securityfocus.com/bid/38552>
- * VUPEN: VUPEN/ADV-2010-0566
<http://www.vupen.com/english/advisories/2010/0566>
- * SECTRACK: 1023698
<http://securitytracker.com/alerts/2010/Mar/1023698.html>
- * MS: MS10-017
<http://www.microsoft.com/technet/security/bulletin/ms10-017.msp>

CVE Reference:

CVE-2010-0261 (cve.mitre.org, nvd.nist.gov)

• **18726 Microsoft Office Excel FNGROUPNAME Record Uninitialized Memory Vulnerability (MS10-017/980150) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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.

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

References:

- * BID: 38553
<http://www.securityfocus.com/bid/38553>
- * VUPEN: VUPEN/ADV-2010-0566
<http://www.vupen.com/english/advisories/2010/0566>
- * SECTRACK: 1023698
<http://securitytracker.com/alerts/2010/Mar/1023698.html>
- * MS: MS10-017
<http://www.microsoft.com/technet/security/bulletin/ms10-017.msp>

CVE Reference:

CVE-2010-0262 (cve.mitre.org, nvd.nist.gov)

• 18727 Microsoft Office Excel XLSX File Parsing Code Execution Vulnerability (MS10-017/980150) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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.

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

References:

- * BID: 38554
<http://www.securityfocus.com/bid/38554>
- * VUPEN: VUPEN/ADV-2010-0566
<http://www.vupen.com/english/advisories/2010/0566>
- * SECTRACK: 1023698
<http://securitytracker.com/alerts/2010/Mar/1023698.html>
- * MS: MS10-017
<http://www.microsoft.com/technet/security/bulletin/ms10-017.msp>

CVE Reference:

CVE-2010-0263 (cve.mitre.org, nvd.nist.gov)

• 18728 Microsoft Office Excel DbOrParamQry Record Parsing Vulnerability (MS10-017/980150) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel 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.

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

References:

- * BID: 38555
<http://www.securityfocus.com/bid/38555>
- * VUPEN: VUPEN/ADV-2010-0566
<http://www.vupen.com/english/advisories/2010/0566>
- * SECTRACK: 1023698
<http://securitytracker.com/alerts/2010/Mar/1023698.html>
- * MS: MS10-017
<http://www.microsoft.com/technet/security/bulletin/ms10-017.msp>

CVE Reference:

CVE-2010-0264 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2010-0257** Microsoft CVSS 2.0 Score = 9.3

Microsoft Office Excel 2002 SP3 does not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Microsoft Office Excel Record Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-017.msp>

CVE Reference: [CVE-2010-0257](#)

• **CVE-2010-0258 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Excel 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Excel Viewer SP1 and SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 do not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Microsoft Office Excel Sheet Object Type Confusion Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-017.msp>

CVE Reference: [CVE-2010-0258](#)

• **CVE-2010-0260 Microsoft CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in Microsoft Office Excel 2007 SP1 and SP2; Office Excel Viewer SP1 and SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Microsoft Office Excel MDXTUPLE Record Heap Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-017.msp>

CVE Reference: [CVE-2010-0260](#)

• **CVE-2010-0261 Microsoft CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in Microsoft Office Excel 2007 SP1 and SP2 and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Microsoft Office Excel MDXSET Record Heap Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-017.msp>

CVE Reference: [CVE-2010-0261](#)

• **CVE-2010-0262 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Excel 2007 SP1 and SP2 and Office 2004 for Mac do not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Microsoft Office Excel FNGROUPNAME Record Uninitialized Memory Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-017.msp>

CVE Reference: [CVE-2010-0262](#)

• **CVE-2010-0263 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Excel 2007 SP1 and SP2; Office 2008 for Mac; Open XML File Format Converter for Mac; Office Excel Viewer SP1 and SP2; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2; and Office SharePoint Server 2007 SP1 and SP2 do not validate ZIP headers during decompression of Open XML (.XLSX) documents, which allows remote attackers to execute arbitrary code via a crafted document that triggers access to uninitialized memory locations, aka "Microsoft Office Excel XLSX File Parsing Code Execution Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-017.msp>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-10-025/>

CVE Reference: [CVE-2010-0263](#)

• **CVE-2010-0264 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Excel 2002 SP3, Office 2004 and 2008 for Mac, and Open XML File Format Converter for Mac do not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Microsoft Office Excel DbOrParamQry Record Parsing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-017.msp>

CVE Reference: [CVE-2010-0264](#)

• **CVE-2010-0265 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in Microsoft Windows Movie Maker 2.1, 2.6, and 6.0, and Microsoft Producer 2003, allows remote attackers to execute arbitrary code via a crafted project (.MSWMM) file, aka "Movie Maker and Producer Buffer Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-016.msp>

CVE Reference: [CVE-2010-0265](#)

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