

2010 Issue #16

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

Live attack using Java hole. Major Zeus botnet activity. .zip's with malware. Rogue anti-virus growing in prevalence.

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

- **Unpatched Java hole exploited at lyrics site**

(Credit: Sun/Oracle)

An unpatched hole in Java was being exploited to target visitors to a song lyrics Web site and more attacks are likely, researchers warned on Wednesday.

The flaw in Java Web Start, disclosed last week by several security researchers, affects Windows systems running Firefox and Internet Explorer, said Roger Thompson, AVG chief research officer. He said he couldn't get it to work on Chrome though, despite reports that it does. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20002530-245.html?part=rss&subj=news&tag=2547-1_3-0-20

- **88 percent of firms show Zeus botnet activity**

Most major U.S. corporations--up to 88 percent of the Fortune 500 companies--may be affected by botnet activity from computers compromised by the Zeus data-stealing Trojan, according to an RSA study released Wednesday.

RSA's FraudAction Anti-Trojan services analyzed data stolen by Zeus from infected computers in August and traced evidence back to IP addresses and e-mail addresses belonging to the corporations, said Sean Brady, manager of the Identity Protection and Verification Group at RSA, which is the security division of EMC.

Specifically, "domains individually representing 88 percent of the Fortune 500 were shown to have been accessed to some extent by computers infected by the Zeus Trojan," the study said. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20002425-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Researchers warn of malware hidden in .zip files

(Credit: Black Hat)

Security researchers have discovered flaws in common file formats, including .zip, which can be used to sneak malware onto computers by evading antivirus detection.

Eight vulnerabilities were found in .zip, supported by Microsoft Office, along with seven others in the .7zip, .rar, .cab and .gzip file formats, said Mario Vuksan, president of ReversingLabs Corp. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20002542-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Google says 11,000 domains distributing rogue anti-virus

Rogue anti-virus software currently accounts for 15 percent of all web-based malware and is growing in prevalence, according to researchers at Google. During the course of a 13-month analysis of fake AV on the web, Google researchers analyzed 240 million web pages collected by the search giant's malware detection engine and found that more than 11,000 domains were involved in the distribution of fake AV.

Google researchers wrote a paper about their findings, which they plan to release April 27 at the Usenix Workshop on Large-Scale Exploits and Emergent Threats in San Jose, Calif. Rogue AV, which currently accounts for 15 percent of all malware Google detects on the web, is rising in prevalence faster than other forms of web-based malware, the company said. SC Magazine

Full Story :

http://www.scmagazineus.com/google-says-11000-domains-distributing-rogue-anti-virus/article/168035/?utm_source

New Vulnerabilities Tested in SecureScout

• 18761 Mozilla Thunderbird - Dangling pointer vulnerability in nsTreeContentView Vulnerability (Remote File Checking)

Security researcher regenrecht reported via TippingPoint's Zero Day Initiative an error in the way <option> elements are inserted into a XUL tree <optgroup>. In certain cases, the number of references to an <option> element is under-counted so that when the element is deleted, a live pointer to its old location is kept around and may later be used. An attacker could potentially use these conditions to run arbitrary code on a victim's computer.

The issue has been fixed in Thunderbird 3.0.4.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2010/mfsa2010-18.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=538308

* FEDORA: FEDORA-2010-5526

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038367.html>

* FEDORA: FEDORA-2010-5539

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/038378.html>

* REDHAT: RHSA-2010:0332

<http://www.redhat.com/support/errata/RHSA-2010-0332.html>

* REDHAT: RHSA-2010:0333

<http://www.redhat.com/support/errata/RHSA-2010-0333.html>

* SECTRACK: 1023776

<http://securitytracker.com/id?1023776>

* SECTRACK: 1023782

<http://securitytracker.com/id?1023782>

* SECUNIA: 38566

<http://secunia.com/advisories/38566>

* SECUNIA: 39117

<http://secunia.com/advisories/39117>

* SECUNIA: 39136

<http://secunia.com/advisories/39136>

* SECUNIA: 39204

<http://secunia.com/advisories/39204>

* SECUNIA: 39240

<http://secunia.com/advisories/39240>

* SECUNIA: 39242

<http://secunia.com/advisories/39242>

* SECUNIA: 39243

<http://secunia.com/advisories/39243>

* VUPEN: ADV-2010-0748

<http://www.vupen.com/english/advisories/2010/0748>

* VUPEN: ADV-2010-0764

<http://www.vupen.com/english/advisories/2010/0764>

* VUPEN: ADV-2010-0765

<http://www.vupen.com/english/advisories/2010/0765>

* XF: firefox-nstreecontentview-code-exec(57392)

<http://xforce.iss.net/xforce/xfdb/57392>

CVE Reference:

CVE-2010-0176 (cve.mitre.org, nvd.nist.gov)

• 18762 WinVerifyTrust Signature Validation Vulnerability (MS10-019/981210) (Remote File Checking)

A remote code execution vulnerability exists in the Windows Authenticode Signature Verification function used for portable executable (PE) and cabinet file formats. An anonymous attacker could exploit the vulnerability by modifying an existing signed executable file to manipulate unverified portions of the signature and file in such a way as to add malicious code to the file without invalidating the signature. 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: MS10-019

<http://www.microsoft.com/technet/security/Bulletin/MS10-019.mspx>

* SECTRACK: 1023846

<http://securitytracker.com/alerts/2010/Apr/1023846.html>

* VUPEN: VUPEN/ADV-2010-0863

<http://www.vupen.com/english/advisories/2010/0863>

* BID: 39328

<http://www.securityfocus.com/bid/39328>

CVE Reference:

CVE-2010-0486 (cve.mitre.org, nvd.nist.gov)

• 18763 Cabview Corruption Validation Vulnerability (MS10-019/981210) (Remote File Checking)

A remote code execution vulnerability exists in the Windows Authenticode Signature verification for cabinet (.cab) file formats. An anonymous attacker could exploit the vulnerability by modifying an existing signed cabinet file to point the unverified portions of the signature to malicious code, and then convincing a user to open or view the specially crafted cabinet 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.

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

References:

* MS: MS10-019

<http://www.microsoft.com/technet/security/Bulletin/MS10-019.mspx>

* SECTRACK: 1023846

<http://securitytracker.com/alerts/2010/Apr/1023846.html>

* VUPEN: VUPEN/ADV-2010-0863
<http://www.vupen.com/english/advisories/2010/0863>
* BID: 39332
<http://www.securityfocus.com/bid/39332>

CVE Reference:

CVE-2010-0487 (cve.mitre.org, nvd.nist.gov)

• **18764 SMB Client Incomplete Response Vulnerability (MS10-020/980232) (Remote File Checking)**

A denial of service vulnerability exists in the way that the Microsoft Server Message Block (SMB) client implementation handles specially crafted SMB responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. An attacker who successfully exploited this vulnerability could cause the computer to stop responding until restarted.

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

References:

* MS: MS10-020
<http://www.microsoft.com/technet/security/Bulletin/MS10-020.mspx>
* SECTRACK: 1023847
<http://securitytracker.com/alerts/2010/Apr/1023847.html>
* VUPEN: VUPEN/ADV-2010-0864
<http://www.vupen.com/english/advisories/2010/0864>
* BID: 36989
<http://www.securityfocus.com/bid/36989>

CVE Reference:

CVE-2009-3676 (cve.mitre.org, nvd.nist.gov)

• **18765 SMB Client Memory Allocation Vulnerability (MS10-020/980232) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that the Microsoft Server Message Block (SMB) client implementation allocates memory when parsing specially crafted SMB responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. An attacker who successfully exploited this vulnerability could execute arbitrary code and 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: MS10-020
<http://www.microsoft.com/technet/security/Bulletin/MS10-020.mspx>
* SECTRACK: 1023847
<http://securitytracker.com/alerts/2010/Apr/1023847.html>
* VUPEN: VUPEN/ADV-2010-0864
<http://www.vupen.com/english/advisories/2010/0864>
* BID: 39312
<http://www.securityfocus.com/bid/39312>

CVE Reference:

CVE-2010-0269 (cve.mitre.org, nvd.nist.gov)

• **18766 SMB Client Transaction Vulnerability (MS10-020/980232) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that the Microsoft Server Message Block (SMB) client implementation handles specially crafted SMB transaction responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. An attacker who successfully exploited this vulnerability could take complete control of the system.

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

References:

* MS: MS10-020
<http://www.microsoft.com/technet/security/Bulletin/MS10-020.mspx>
* SECTRACK: 1023847

<http://securitytracker.com/alerts/2010/Apr/1023847.html>

* VUPEN: VUPEN/ADV-2010-0864

<http://www.vupen.com/english/advisories/2010/0864>

* BID: 39339

<http://www.securityfocus.com/bid/39339>

CVE Reference:

CVE-2010-0270 (cve.mitre.org, nvd.nist.gov)

• **18767 SMB Client Response Parsing Vulnerability (MS10-020/980232) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that the Microsoft Server Message Block (SMB) client implementation parses specially crafted SMB transaction responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. An attacker who successfully exploited this vulnerability could take complete control of the system.

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

References:

* MS: MS10-020

<http://www.microsoft.com/technet/security/Bulletin/MS10-020.mspx>

* SECTRACK: 1023847

<http://securitytracker.com/alerts/2010/Apr/1023847.html>

* VUPEN: VUPEN/ADV-2010-0864

<http://www.vupen.com/english/advisories/2010/0864>

* BID: 39336

<http://www.securityfocus.com/bid/39336>

CVE Reference:

CVE-2010-0476 (cve.mitre.org, nvd.nist.gov)

• **18768 SMB Client Message Size Vulnerability (MS10-020/980232) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that the Microsoft Server Message Block (SMB) client implementation handles specially crafted SMB responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. An attacker who successfully exploited this vulnerability could take complete control of the system.

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

References:

* MS: MS10-020

<http://www.microsoft.com/technet/security/Bulletin/MS10-020.mspx>

* SECTRACK: 1023847

<http://securitytracker.com/alerts/2010/Apr/1023847.html>

* VUPEN: VUPEN/ADV-2010-0864

<http://www.vupen.com/english/advisories/2010/0864>

* BID: 39340

<http://www.securityfocus.com/bid/39340>

CVE Reference:

CVE-2010-0477 (cve.mitre.org, nvd.nist.gov)

• **18769 Visio Attribute Validation Memory Corruption Vulnerability (MS10-028/980094) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Visio validates attributes when handling specially crafted Visio 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 affected than users who operate with administrative user rights.

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

References:

* MS: MS10-028
<http://www.microsoft.com/technet/security/Bulletin/MS10-028.msp>
* SECTRACK: 1023856
<http://securitytracker.com/alerts/2010/Apr/1023856.html>
* VUPEN: VUPEN/ADV-2010-0871
<http://www.vupen.com/english/advisories/2010/0871>
* BID: 39300
<http://www.securityfocus.com/bid/39300>

CVE Reference:

CVE-2010-0254 (cve.mitre.org, nvd.nist.gov)

• **18770 Visio Index Calculation Memory Corruption Vulnerability (MS10-028/980094) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Visio calculates indexes when handling specially crafted Visio 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 affected than users who operate with administrative user rights.

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

References:

* MS: MS10-028
<http://www.microsoft.com/technet/security/Bulletin/MS10-028.msp>
* SECTRACK: 1023856
<http://securitytracker.com/alerts/2010/Apr/1023856.html>
* VUPEN: VUPEN/ADV-2010-0871
<http://www.vupen.com/english/advisories/2010/0871>
* BID: 39302
<http://www.securityfocus.com/bid/39302>

CVE Reference:

CVE-2010-0256 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2010-0254 Microsoft CVSS 2.0 Score = 7.6**

Microsoft Office Visio 2002 SP2, 2003 SP3, and 2007 SP1 and SP2 does not properly validate attributes in Visio files, which allows remote attackers to execute arbitrary code via a crafted file, aka "Visio Attribute Validation Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-028.msp>

CVE Reference: [CVE-2010-0254](http://cve.mitre.org)

• **CVE-2010-0256 Microsoft CVSS 2.0 Score = 7.6**

Microsoft Office Visio 2002 SP2, 2003 SP3, and 2007 SP1 and SP2 does not properly calculate unspecified indexes associated with Visio files, which allows remote attackers to execute arbitrary code via a crafted file, aka "Visio Index Calculation Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-028.msp>

CVE Reference: [CVE-2010-0256](http://cve.mitre.org)

• **CVE-2010-0237 Microsoft CVSS 2.0 Score = 6.9**

The kernel in Microsoft Windows 2000 SP4 and XP SP2 and SP3 allows local users to gain privileges by creating a symbolic link from an untrusted registry hive to a trusted registry hive, aka "Windows Kernel Symbolic Link Creation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>

CVE Reference: [CVE-2010-0237](#)

• **CVE-2010-0236 Microsoft CVSS 2.0 Score = 6.8**

The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Vista Gold does not properly allocate memory for the destination key associated with a symbolic-link registry key, which allows local users to gain privileges via a crafted application, aka "Windows Kernel Memory Allocation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>

CVE Reference: [CVE-2010-0236](#)

• **CVE-2010-0024 Microsoft CVSS 2.0 Score = 5.0**

The SMTP component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Server 2008 Gold, SP2, and R2, and Exchange Server 2003 SP2, does not properly parse MX records, which allows remote DNS servers to cause a denial of service (service outage) via a crafted response to a DNS MX record query, aka "SMTP Server MX Record Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-024.msp>

CVE Reference: [CVE-2010-0024](#)

• **CVE-2010-0025 Microsoft CVSS 2.0 Score = 5.0**

The SMTP component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Server 2008 Gold, SP2, and R2, and Exchange Server 2000 SP3, does not properly allocate memory for SMTP command replies, which allows remote attackers to read fragments of e-mail messages by sending a series of invalid commands and then sending a STARTTLS command, aka "SMTP Memory Allocation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-024.msp>

CVE Reference: [CVE-2010-0025](#)

• **CVE-2010-0238 Microsoft CVSS 2.0 Score = 4.9**

Unspecified vulnerability in registry-key validation in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Vista Gold allows local users to cause a denial of service (reboot) via a crafted application, aka "Windows Kernel Registry Key Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>

CVE Reference: [CVE-2010-0238](#)

• **CVE-2010-0888 Oracle CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the Sun Ray Server Software component in Oracle Sun Product Suite 4.0, 4.1, and 4.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Device Services.

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

References:

CONFIRM: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-274590-1>

CVE Reference: [CVE-2010-0888](https://cve.mitre.org/cve/2010/0888)

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