

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

Another certificate authority breached. SpyEye targeting Android. Large gain from hacking. But crime doesn't pay.

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

• GlobalSign discovers "isolated" web server compromise

Portsmouth, N.H.-based certificate authority (CA) GlobalSign has discovered that the web server hosting its site was compromised by hackers, the company announced late Friday. "The breached web server has always been isolated from all other infrastructure and is used only to serve the www.globalsign.com website," GlobalSign said in a news release. "At present there is no further evidence of breach other than the isolated [www](http://www.globalsign.com) web server."

The company said it is closely monitoring all activity to its services in light of what it deems an "industry-wide" attack against CAs.

Last week, GlobalSign temporarily suspended its issuing of SSL credentials due to claims from a hacker linked to recent attacks on CAs Comodo and DigiNotar. The so-called Comodohacker claimed responsibility for the recent attack on DigiNotar and said he has access to four other CAs, including GlobalSign. SC Magazine

Full Story :

http://www.scmagazineus.com/globalsign-discovers-isolated-web-server-compromise/article/211907/?utm_source=f

• **Android OS under attack from new trojan variant**

A variant of the SpyEye trojan is targeting the Google Android operating system, security firm Trusteer announced on its blog on Tuesday.

The original SpyEye trojan was found by Trusteer researchers in July to be collecting personal and banking information across the globe. At the time, researchers said the malware was capable of evading transaction monitoring systems that look for anomalies, and observed new variants appearing frequently.

The newest version, dubbed SpitMo (SpyEye for mobile), was first detected in April by security firm F-Secure. SC Magazine

Full Story :

http://www.scmagazineus.com/android-os-under-attack-from-new-trojan-variant/article/211927/?utm_source=feedbu

• **Hacker "soldier" steals \$3.2 million from U.S. companies**

A hacker known in the cybercriminal underground as "soldier" has stolen \$3.2 million from major U.S. corporations in the past six months, according to researchers at anti-virus firm Trend Micro. The attacker, believed to be in his early 20s and residing in Russia, used various toolkits, such as SpyEye and Zeus, to plunder millions of dollars from corporate bank accounts since January, Jamz Yaneza, threat research manager at Trend Micro, told SCMagazineUS.com on Thursday. The hacker oversees a network of money mules and accomplices, who are believed to reside in West Hollywood and Venice, Calif.

Trend researchers have been investigating the hacker's operations since April and have notified federal authorities, Yaneza said. SC Magazine

Full Story :

http://www.scmagazineus.com/hacker-soldier-steals-32-million-from-us-companies/article/212070/?utm_source=feed

• **Online ID thief sentenced to 14 years**

A man who pleaded guilty on April 4 to one count of wire fraud and one count of aggravated identity theft was sentenced last week in U.S. District Court in Alexandria, Va. to 14 years in prison. Tony Perez III, 21, of Hammond, Ind., stood accused of running a business online that sold counterfeit credit cards embedded with account information purloined from various sources. The sentencing announcement was made on Friday by Assistant Attorney General Lanny A. Breuer of the Criminal Division and U.S. Attorney Neil H. MacBride for the Eastern District of Virginia.

Perez used a number of online identities in underground discussion groups which facilitated a market for stolen financial account information, according to court documents. SC Magazine

Full Story :

http://www.scmagazineus.com/online-id-thief-sentenced-to-14-years/article/211853/?utm_source=feedburner&utm_m

New Vulnerabilities Tested in SecureScout

• **19461 phpMyAdmin code injection vulnerability in setup.php**

phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW.

Static code injection vulnerability in setup.php in phpMyAdmin 2.11.x before 2.11.9.5 and 3.x before 3.1.3.1 allows remote attackers to inject arbitrary PHP code into a configuration file via the save action.

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

References:

* BUGTRAQ: 20090609 CVE-2009-1151: phpMyAdmin Remote Code Execution Proof of Concept

<http://www.securityfocus.com/archive/1/archive/1/504191/100/0/threaded>

* MISC:

<http://labs.neohapsis.com/2009/04/06/about-cve-2009-1151/>

* MISC:

<http://www.gnucitizen.org/blog/cve-2009-1151-phpmyadmin-remote-code-execution-proof-of-concept/>

* CONFIRM:

http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin/branches/MAINT_2_11_9/phpMyAdmin/scripts/setup.php?r1

* CONFIRM:

http://www.phpmyadmin.net/home_page/security/PMASA-2009-3.php

* DEBIAN: DSA-1824

<http://www.debian.org/security/2009/dsa-1824>

* GENTOO: GLSA-200906-03

<http://security.gentoo.org/glsa/glsa-200906-03.xml>

* MANDRIVA: MDVSA-2009:115

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:115>

* SUSE: SUSE-SR:2009:008

<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00003.html>

* BID: 34236

<http://www.securityfocus.com/bid/34236>

* SECUNIA: 34430

<http://secunia.com/advisories/34430>

* SECUNIA: 34642

<http://secunia.com/advisories/34642>

* SECUNIA: 35585

<http://secunia.com/advisories/35585>

* SECUNIA: 35635

<http://secunia.com/advisories/35635>

CVE Reference:

CVE-2009-1151 (cve.mitre.org, nvd.nist.gov)

• 19462 Excel Use after Free WriteAV Vulnerability (MS11-072/2587505) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft 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:

* MS: ms11-072

<http://technet.microsoft.com/en-us/security/bulletin/ms11-072>

* BID: 49476

<http://www.securityfocus.com/bid/49476>

* SECTRACK: 1026038

<http://www.securitytracker.com/id/1026038>

CVE Reference:

CVE-2011-1986 (cve.mitre.org, nvd.nist.gov)

• 19463 Excel Out of Bounds Array Indexing Vulnerability (MS11-072/2587505) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft 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:

* MS: ms11-072

<http://technet.microsoft.com/en-us/security/bulletin/ms11-072>

* BID: 49477

<http://www.securityfocus.com/bid/49477>

* SECTRACK: 1026038

<http://www.securitytracker.com/id/1026038>

CVE Reference:

CVE-2011-1987 (cve.mitre.org, nvd.nist.gov)

• 19464 Excel Heap Corruption Vulnerability (MS11-072/2587505) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft 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:

* MS: ms11-072

<http://technet.microsoft.com/en-us/security/bulletin/ms11-072>

* BID: 49478

<http://www.securityfocus.com/bid/49478>

* SECTRACK: 1026038

<http://www.securitytracker.com/id/1026038>

CVE Reference:

CVE-2011-1988 (cve.mitre.org, nvd.nist.gov)

• **19465 Excel Conditional Expression Parsing Vulnerability (MS11-072/2587505) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft 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:

* MS: ms11-072

<http://technet.microsoft.com/en-us/security/bulletin/ms11-072>

* BID: 49518

<http://www.securityfocus.com/bid/49518>

* SECTRACK: 1026038

<http://www.securitytracker.com/id/1026038>

CVE Reference:

• **19466 Excel Out of Bounds Array Indexing Vulnerability (CVE-2011-1990) (MS11-072/2587505) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft 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:

* MS: ms11-072

<http://technet.microsoft.com/en-us/security/bulletin/ms11-072>

* BID: 49517

<http://www.securityfocus.com/bid/49517>

* SECTRACK: 1026038

<http://www.securitytracker.com/id/1026038>

CVE Reference:

CVE-2011-1990 (cve.mitre.org, nvd.nist.gov)

• **19467 Office Component Insecure Library Loading Vulnerability (MS11-073/2587634) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office 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:

* MS: ms11-073

<http://technet.microsoft.com/en-us/security/bulletin/ms11-073>

* BID: 49519

<http://www.securityfocus.com/bid/49519>

* SECTRACK: 1026039

<http://www.securitytracker.com/id/1026039>

CVE Reference:

CVE-2011-1980 (cve.mitre.org, nvd.nist.gov)

• **19468 Office Uninitialized Object Pointer Vulnerability (MS11-072/2587505) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles specially crafted Word 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:

- * MS: ms11-073
<http://technet.microsoft.com/en-us/security/bulletin/ms11-073>
- * BID: 49513
<http://www.securityfocus.com/bid/49513>
- * SECTRACK: 1026039
<http://www.securitytracker.com/id/1026039>

CVE Reference:

CVE-2011-1982 (cve.mitre.org, nvd.nist.gov)

• 19469 WINS Local Elevation of Privilege Vulnerability(MS11-070/2571621) (Remote File Checking)

An elevation of privilege vulnerability exists in WINS, allowing arbitrary code to be executed in the context of the local system. The vulnerability is caused when the WINS server improperly processes a sequence of specially crafted packets received on the loopback interface. A local attacker who successfully exploited this vulnerability could execute arbitrary code and take complete control of an affected system. The 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: ms11-070
<http://technet.microsoft.com/en-us/security/bulletin/ms11-070>
- * BID: 49523
<http://www.securityfocus.com/bid/49523>
- * SECTRACK: 1026037
<http://www.securitytracker.com/id/1026037>

CVE Reference:

CVE-2011-1984 (cve.mitre.org, nvd.nist.gov)

• 19470 Windows Components Insecure Library Loading Vulnerability (MS11-071/2570947) (Remote File Checking)

A remote code execution vulnerability exists in the way that certain Windows components handle 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:

- * MS: ms11-071
<http://technet.microsoft.com/en-us/security/bulletin/ms11-071>
- * BID: 47741
<http://www.securityfocus.com/bid/47741>
- * SECTRACK: 1026041
<http://www.securitytracker.com/id/1026041>

CVE Reference:

CVE-2011-1991 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-1980 Microsoft CVSS 2.0 Score = 9.3

Untrusted search path vulnerability in Microsoft Office 2003 SP3 and 2007 SP2 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .doc, .ppt, or .xls file, aka "Office Component Insecure Library Loading Vulnerability." Per: <http://cwe.mitre.org/data/definitions/426.html>

'CWE-426: Untrusted Search Path'

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-073>

CVE Reference: [CVE-2011-1980](#)

• **CVE-2011-1982 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office 2007 SP2, and 2010 Gold and SP1, does not initialize an unspecified object pointer during the opening of Word documents, which allows remote attackers to execute arbitrary code via a crafted document, aka "Office Uninitialized Object Pointer Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-073>

CVE Reference: [CVE-2011-1982](#)

• **CVE-2011-1986 Microsoft CVSS 2.0 Score = 9.3**

Use-after-free vulnerability in Microsoft Excel 2003 SP3 allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel Use after Free WriteAV Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-072>

CVE Reference: [CVE-2011-1986](#)

• **CVE-2011-1987 Microsoft CVSS 2.0 Score = 9.3**

Array index error in Microsoft Excel 2003 SP3 and 2007 SP2; Excel in Office 2007 SP2; Excel 2010 Gold and SP1; Excel in Office 2010 Gold and SP1; Office 2004, 2008, and 2011 for Mac; Open XML File Format Converter for Mac; Excel Viewer SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP2 allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel Out of Bounds Array Indexing Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-072>

CVE Reference: [CVE-2011-1987](#)

• **CVE-2011-1988 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Excel 2003 SP3 and 2007 SP2; Excel in Office 2007 SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Excel Viewer SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP2 do not properly parse records in Excel spreadsheets, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel Heap Corruption Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-072>

CVE Reference: [CVE-2011-1988](#)

• **CVE-2011-1989 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Excel 2003 SP3 and 2007 SP2; Excel in Office 2007 SP2; Excel 2010 Gold and SP1; Excel in Office 2010 Gold and SP1; Office 2004, 2008, and 2011 for Mac; Open XML File Format Converter for Mac; Excel Viewer SP2; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP2; Excel Services on Office SharePoint Server 2007 SP2; Excel Services on Office SharePoint Server 2010 Gold and SP1; and Excel Web App 2010 Gold and SP1 do not properly parse conditional expressions associated with formatting requirements, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel Conditional Expression Parsing Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-072>

CVE Reference: [CVE-2011-1989](#)

• **CVE-2011-1990 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Excel 2007 SP2; Excel in Office 2007 SP2; Excel Viewer SP2; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP2; and Excel Services on Office SharePoint Server 2007 SP2 do not properly validate the sign of an unspecified array index, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel Out of Bounds Array Indexing Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-072>

CVE Reference: [CVE-2011-1990](#)

• **CVE-2011-1991 Microsoft CVSS 2.0 Score = 9.3**

Multiple untrusted search path vulnerabilities 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 allow local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .doc, .rtf, or .txt file, related to (1) deskpan.dll in the Display Panning CPL Extension, (2) EAPHost Authenticator Service, (3) Folder Redirection, (4) HyperTerminal, (5) the Japanese Input Method Editor (IME), and (6) Microsoft Management Console (MMC), aka "Windows Components Insecure Library Loading Vulnerability."Per: <http://cwe.mitre.org/data/definitions/426.html>'CWE-426: Untrusted Search Path'

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-071>

CVE Reference: [CVE-2011-1991](#)

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