

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

Australia wins SANS security award. Many businesses victims of the RSA attack. SMS Trojans with shared code. Sudden increase in bank phishing.

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

• Australian gov't wins U.S. security award from SANS

Australia's Defense Signals Directorate (DSD), a government intelligence agency, has won a security award for setting security standards that are cheaper and more effective than those in place at U.S. government agencies.

It won the U.S. National Cybersecurity Innovation Award from the SANS Institute for "groundbreaking innovation" in four basic security controls and 35 others that help mitigate breaches.

The four controls - application updating and patching; operating system patching; whitelisting, and strict account control - were derived from research into security intrusions in military and civilian IT systems. SC Magazine

Full Story :

http://www.scmagazineus.com/australian-govt-wins-us-security-award-from-sans/article/215403/?utm_source=feedb

• Report: RSA hackers knock off 760 other businesses

At least 760 organizations appear to have fallen victim to the same attacks that compromised RSA's SecurID authentication system earlier this year.

The names appear on a list of targeted machines that had phoned home to the same command-and-control (C&C) servers used in the March attacks on RSA. The list was shared by information professionals to Congress and subsequently published by blog "Krebs on Security."

It includes names such as eBay, Motorola, IBM, McAfee and VMware. A number of telecommunication firms also appeared on the list but likely because their subscribers were compromised. SC Magazine

Full Story :

http://www.scmagazineus.com/report-rsa-hackers-knock-off-760-other-businesses/article/215238/?utm_source=feed

• Premium-rate SMS trojan shares code with SpyEye variant

Researchers have discovered a group of premium-rate SMS trojans that share code with Spitmo, a mobile variant of the notorious banking trojan SpyEye, according to F-Secure. The so-called "cousins of Spitmo" are premium-rate SMS trojans that target Russian users of Symbian and Windows Mobile phones, Sean Sullivan, security adviser at F-Secure, told SCMagazineUS.com on Thursday. The malware was named OpFake because the installer purports to be an updater for Opera Mini, a mobile web browser.

Once installed on a victim's phone, OpFake sends SMS messages to Russian-based premium-rate numbers without the owner's consent, Sullivan said. The malware then prevents messages that verify the text went through from being sent back to the user's phone.

The source code used to intercept incoming messages is nearly identical to that in Spitmo. SC Magazine

Full Story :

http://www.scmagazineus.com/premium-rate-sms-trojan-shares-code-with-spyeye-variant/article/215429/?utm_source=feed

• Banker trade group warns of phishing uptick

The American Bankers Association (ABA) on Wednesday issued a new warning about a "sudden increase" in phishing scams being reported throughout the country. Online miscreants are using automated dialers, text messages and emails to trick users into believing their accounts have been closed due to fraud, according to the alert. Users are subsequently directed to enter their credit card information, including expiration number and CV security code, to reactivate their account.

Cybercriminals typically ramp up their phishing efforts during the end of the year holiday season and following natural disasters, Doug Johnson, vice president of risk management policy at ABA, told SCMagazineUS.com on Thursday.

"Customer education is an ongoing process and it's good to periodically remind users that the threat exists and they need to protect themselves," Johnson said. SC Magazine

Full Story :

http://www.scmagazineus.com/banker-trade-group-warns-of-phishing-uptick/article/215440/?utm_source=feedburner

New Vulnerabilities Tested in SecureScout

• 19540 Microsoft .NET Framework 'System.Net.Sockets' Namespace Security Bypass Vulnerability (MS11-069/2567951) (Remote File Checking)

The Microsoft .NET Framework is prone to a security-bypass vulnerability.

The vulnerability could allow information disclosure if a user views a specially crafted Web page using a Web browser that can run XAML Browser Applications (XBAPs). In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site. This vulnerability could also be used by Windows .NET applications to bypass Code Access Security (CAS) restrictions.

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

References:

* MS: MS11-069

<http://www.microsoft.com/technet/security/Bulletin/MS11-069.msp>

* OVAL: oval:org.mitre.oval:def:12901

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12901>

* BID: 48991

<http://www.securityfocus.com/bid/48991/info>

CVE Reference:

CVE-2011-1978 (cve.mitre.org, nvd.nist.gov)

• 19541 Microsoft Windows Active Accessibility DLL Loading Arbitrary Code Execution Vulnerability (MS11-075/2623699) (Remote File Checking)

Microsoft Windows is prone to an arbitrary-code-execution vulnerability that affects the Active Accessibility component.

The vulnerability could allow remote code execution if an attacker convinces a user to open a legitimate file that is located in the same network directory as a specially crafted dynamic link library (DLL) file. Then, while opening the legitimate file, the Microsoft Active Accessibility component could attempt to load the DLL file and execute any code it contained. For an attack to be successful, a user must visit an untrusted remote file system location or WebDAV share and open a document from this location that is then loaded by a vulnerable application.

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

References:

* MS: MS11-075

<http://technet.microsoft.com/en-us/security/bulletin/MS11-075>

* BID: 49975

<http://www.securityfocus.com/bid/49976/info>

* MISC: CVE-2011-1247

<http://www.security-database.com/detail.php?alert=CVE-2011-1247>

CVE Reference:

CVE-2011-1247 (cve.mitre.org, nvd.nist.gov)

• 19542 Microsoft Windows Media Center DLL Loading Arbitrary Code Execution Vulnerability (MS11-076/2604926) (Remote File Checking)

Microsoft Windows is prone to an arbitrary-code-execution vulnerability that affects the Media Center.

The vulnerability could allow remote code execution if an attacker convinces a user to open a legitimate file that is located in the same network directory as a specially crafted dynamic link library (DLL) file. Then, while opening the legitimate file, Windows Media Center could attempt to load the DLL file and execute any code it contained. For an attack to be successful, a user must visit an untrusted remote file system location or WebDAV share and open a legitimate file.

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

References:

* MS: MS11-076

<http://technet.microsoft.com/en-us/security/bulletin/MS11-076>

* BID: 49943

<http://www.securityfocus.com/bid/49943/info>

CVE Reference:

CVE-2011-2009 (cve.mitre.org, nvd.nist.gov)

• 19543 Microsoft Windows Kernel 'Win32k.sys' Local Privilege Escalation Vulnerability (MS11-077/2567053) (Remote File Checking)

Microsoft Windows is prone to a local privilege-escalation vulnerability that occurs in the Windows kernel due to a NULL-pointer dereference error.

win32k.sys in the kernel-mode drivers 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 does not properly validate user-mode input, which allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application, aka "Win32k Null Pointer De-reference Vulnerability."

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

References:

* MS: MS11-077

<http://technet.microsoft.com/en-us/security/bulletin/MS11-077>

* SECTRACK: 1026165
<http://www.securitytracker.com/id?1026165>
* BID: 49968
<http://www.securityfocus.com/bid/49968/info>

CVE Reference:

CVE-2011-1985 (cve.mitre.org, nvd.nist.gov)

● **19544 Microsoft Windows Kernel 'Win32k.sys' TrueType Font File Remote Denial of Service Vulnerability (MS11-077/2567053) (Remote File Checking)**

Microsoft Windows is prone to a remote denial-of-service vulnerability.

A remote attacker can exploit this issue to crash the Windows kernel, denying service to legitimate users.

win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle TrueType fonts, which allows local users to cause a denial of service (system hang) via a crafted font file, aka "Win32k TrueType Font Type Translation Vulnerability."

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

References:

* MS: MS11-077
<http://technet.microsoft.com/en-us/security/bulletin/MS11-077>
* SECTRACK: 1026165
<http://www.securitytracker.com/id?1026165>
* BID: 49973
<http://www.securityfocus.com/bid/49973/info>

CVE Reference:

CVE-2011-2002 (cve.mitre.org, nvd.nist.gov)

● **19545 Microsoft Windows Kernel '.fon' Font File Remote Code Execution Vulnerability (MS11-077/2567053) (Remote File Checking)**

Buffer overflow in win32k.sys in the kernel-mode drivers 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 allows remote attackers to execute arbitrary code via a crafted .fon file, aka "Font Library File Buffer Overrun Vulnerability."

An attacker can exploit this issue by tricking an unsuspecting victim into viewing a malformed file on a remote network share.

Successful exploits can allow attackers to execute arbitrary code with kernel-level privileges. Failed exploit attempts will result in a denial-of-service condition

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

References:

* MS: MS11-077
<http://technet.microsoft.com/en-us/security/bulletin/MS11-077>
* SECTRACK: 1026165
<http://www.securitytracker.com/id?1026165>
* BID: 49975
<http://www.securityfocus.com/bid/49975/discuss>

CVE Reference:

CVE-2011-2003 (cve.mitre.org, nvd.nist.gov)

● **19546 Microsoft Windows Kernel 'Win32k.sys' Local Privilege Escalation Vulnerability (MS11-077/2567053) (Remote File Checking)**

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers 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 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, aka "Win32k Use After Free Vulnerability."

A local attacker can exploit this issue to execute arbitrary code with kernel-level privileges. Successful exploits will result in the complete compromise of affected computers. Failed exploit attempts may cause a denial-of-service condition.

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

References:

- * MS: MS11-077
<http://technet.microsoft.com/en-us/security/bulletin/MS11-077>
- * SECTRACK: 1026165
<http://www.securitytracker.com/id?1026165>
- * BID: 49981
<http://www.securityfocus.com/bid/49981/info>

CVE Reference:

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

● **19548 Microsoft Windows AFD Driver Local Privilege Escalation Vulnerability (MS11-080/2592799) (Remote File Checking)**

Microsoft Windows is prone to a local privilege-escalation vulnerability.

The vulnerability could allow elevation of privilege if an attacker logs on to a user's system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit the vulnerability. Failed exploit attempts may cause a denial-of-service condition.

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

References:

- * MS: MS11-080
<http://technet.microsoft.com/en-us/security/bulletin/MS11-080>
- * BID: 49941
<http://www.securityfocus.com/bid/49941/info>

CVE Reference:

CVE-2011-2005 (cve.mitre.org, nvd.nist.gov)

● **19549 Microsoft Forefront UAG ExcelTable Response Splitting XSS Vulnerability (MS11-079/2544641) (Remote File Checking)**

Microsoft Forefront Unified Access Gateway is prone to an HTTP response-splitting vulnerability because it fails to sufficiently sanitize user-supplied data.

Attackers can leverage this issue to influence or misrepresent how web content is served, cached, or interpreted. This could aid in conducting cross-site scripting attacks and various other attacks that try to entice client users into a false sense of trust.

CRLF injection vulnerability in Microsoft Forefront Unified Access Gateway (UAG) 2010 Gold, Update 1, Update 2, and SP1 allows remote attackers to inject arbitrary HTTP headers, and conduct HTTP response splitting attacks and cross-site scripting (XSS) attacks, via unspecified vectors, aka "ExcelTable Response Splitting XSS Vulnerability."

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

References:

- * MS: MS11-079
<http://technet.microsoft.com/en-us/security/bulletin/MS11-079>
- * OSVDB: 76235
<http://osvdb.org/76235>
- * BID: 49979
<http://www.securityfocus.com/bid/49979/info>

CVE Reference:

CVE-2011-1895 (cve.mitre.org, nvd.nist.gov)

● **19550 Microsoft Forefront UAG Cross-Site Scripting Vulnerability (MS11-079/2544641) (Remote File Checking)**

Microsoft Forefront Unified Access Gateway is prone to a cross-site scripting vulnerability because Web Monitor fails to properly sanitize user-supplied input.

Cross-site scripting (XSS) vulnerability in Microsoft Forefront Unified Access Gateway (UAG) 2010 Gold, Update 1, Update 2, and SP1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "ExcelTable Reflected XSS Vulnerability."

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may help the attacker steal potentially sensitive information and launch other attacks.

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

References:

- * MS: MS11-079
<http://technet.microsoft.com/en-us/security/bulletin/MS11-079>
- * OSVDB: 76233
<http://osvdb.org/76233>
- * BID: 49972
<http://www.securityfocus.com/bid/49972/info>

CVE Reference:

CVE-2011-1896 (cve.mitre.org, nvd.nist.gov)

• 19551 Microsoft Forefront UAG Null Session Cookie Denial of Service Vulnerability (MS11-079/2544641) (Remote File Checking)

Microsoft Forefront Unified Access Gateway is prone to a remote denial-of-service vulnerability.

Attackers can exploit this issue to crash the web server of the affected application, denying service to legitimate users.

Microsoft Forefront Unified Access Gateway (UAG) 2010 Gold, Update 1, Update 2, and SP1 does not properly validate session cookies, which allows remote attackers to cause a denial of service (IIS outage) via unspecified network traffic, aka "Null Session Cookie Crash."

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

References:

- * MS: MS11-079
<http://technet.microsoft.com/en-us/security/bulletin/MS11-079>
- * BID: 49980
<http://www.securityfocus.com/bid/49980>

CVE Reference:

CVE-2011-2012 (cve.mitre.org, nvd.nist.gov)

• 19552 Microsoft Forefront UAG 'MicrosoftClient.Jar' Remote Code Execution Vulnerability (MS11-079/2544641) (Remote File Checking)

Microsoft Forefront Unified Access Gateway is prone to a remote code-execution vulnerability.

Successful exploits will allow attackers to execute arbitrary code in the context of the logged-in user.

Microsoft Forefront Unified Access Gateway (UAG) 2010 Gold, Update 1, Update 2, and SP1 provides the MicrosoftClient.jar file containing a signed Java applet, which allows remote attackers to execute arbitrary code on client machines via unspecified vectors, aka "Poisoned Cup of Code Execution Vulnerability."

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

References:

- * MS: MS11-079
<http://technet.microsoft.com/en-us/security/bulletin/MS11-079>
- * BID: 49983
<http://www.securityfocus.com/bid/49983>

CVE Reference:

CVE-2011-1969 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-3163 HP CVSS 2.0 Score = 1.2

HP MFP Digital Sending Software 4.9x through 4.91.21 allows local users to obtain sensitive workflow-metadata information via unspecified vectors.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

HP: <http://marc.info/?l=bugtraq&m=131914362310845&w=2>

HP: <http://marc.info/?l=bugtraq&m=131914362310845&w=2>

CVE Reference: [CVE-2011-3163](#)

• **CVE-2011-4171 IBM CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in content/error.jsp in IBM WebSphere ILOG Rule Team Server 7.1.1 allows remote attackers to inject arbitrary web script or HTML via the project parameter to teamsrver/faces/home.jsp.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/70461>

BID: <http://www.securityfocus.com/bid/50056>

OSVDB: <http://www.osvdb.org/76238>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1RS00803>

SECTRACK: <http://securitytracker.com/id?1026170>

SECUNIA: <http://secunia.com/advisories/46350>

CVE Reference: [CVE-2011-4171](#)

• **CVE-2011-2656 Novell CVSS 2.0 Score = 9.3**

Unspecified vulnerability in ZfHSrvr.exe in Novell ZENworks Handheld Management (ZHM) 7 allows remote attackers to execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-2655.

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

References:

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=7009489>

CONFIRM: <http://download.novell.com/Download?buildid=Fz0LYfG9qCU%7E>

XF: <http://xforce.iss.net/xforce/xfdb/70831>

BID: <http://www.securityfocus.com/bid/50303>

CVE Reference: [CVE-2011-2656](#)

• **CVE-2011-2655 Novell CVSS 2.0 Score = 9.3**

Unspecified vulnerability in ZfHSrvr.exe in Novell ZENworks Handheld Management (ZHM) 7 allows remote attackers to execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-2656.

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

References:

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=7009489>

CONFIRM: <http://download.novell.com/Download?buildid=Fz0LYfG9qCU%7E>

XF: <http://xforce.iss.net/xforce/xfdb/70831>

BID: <http://www.securityfocus.com/bid/50303>

CVE Reference: [CVE-2011-2655](#)

• **CVE-2011-1478 Linux CVSS 2.0 Score = 5.7**

The napi_reuse_skb function in net/core/dev.c in the Generic Receive Offload (GRO) implementation in the Linux kernel before 2.6.38 does not reset the values of certain structure members, which might allow remote attackers to

cause a denial of service (NULL pointer dereference) via a malformed VLAN frame.Per:
<http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

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

References:

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=6d152e23ad1a7a5b40fef1f42e017d66e6115159>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=66c46d741e2e60f0e8b625b80edb0ab820c46d7a>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=691270

CONFIRM: <http://www.vmware.com/security/advisories/VMSA-2011-0012.html>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/520102/100/0/threaded>

SECUNIA: <http://secunia.com/advisories/46397>

MLIST: <http://openwall.com/lists/oss-security/2011/03/28/1>

CONFIRM: <http://mirror.anl.gov/pub/linux/kernel/v2.6/ChangeLog-2.6.38>

CVE Reference: [CVE-2011-1478](#)

• **CVE-2011-3891 Google CVSS 2.0 Score = 7.5**

Google Chrome before 15.0.874.102 does not properly restrict access to internal Google V8 functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

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

References:

CONFIRM: <http://googlechromereleases.blogspot.com/2011/10/chrome-stable-release.html>

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=100322>

CVE Reference: [CVE-2011-3891](#)

• **CVE-2011-3890 Google CVSS 2.0 Score = 7.5**

Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to video source handling.

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

References:

CONFIRM: <http://googlechromereleases.blogspot.com/2011/10/chrome-stable-release.html>

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=99553>

CVE Reference: [CVE-2011-3890](#)

• **CVE-2011-3889 Google CVSS 2.0 Score = 7.5**

Heap-based buffer overflow in the Web Audio implementation in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

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

References:

CONFIRM: <http://googlechromereleases.blogspot.com/2011/10/chrome-stable-release.html>

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=99211>

CVE Reference: [CVE-2011-3889](#)

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