

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>

[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

Social network attacks growing. Financial hacker gets 13 years. Olympic tragedy used to spread malware. Fake antivirus program offers 'tech support'.

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

• Malware and social network attacks surge in '09

Malware-carrying spam and attacks via Twitter and Facebook grew dramatically in the second half of 2009, says a report (PDF) released Tuesday by security company M86 Security.

The volume of spam shot up last year to more than 200 billion messages each day, or 80 percent to 90 percent of all inbound e-mail sent to organizations, said M86. Spam carrying malware also surged in the second half of the year, hitting 3 billion each day compared with 600 million per day in the first half of 2009.

The vast majority of spam is now sent through botnets hiding on infected computers--the second half of 2009 alone saw 78 percent of all spam triggered by the top five botnets, such as Rustock and Pushdo. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-10454870-83.html?part=rss&subj=news&tag=2547-1_3-0-20

• 13 years in prison cometh for the "Iceman" hacker

A San Francisco man charged with hacking into financial institutions and then hawking the stolen data in an online forum has been sentenced to 13 years in federal prison.

Max Ray Butler, who uses the online alias "Iceman," additionally was ordered to pay \$27.5 million in restitution. He was sentenced Friday in U.S. District Court in Pittsburgh.

The 37-year-old was indicted in 2007 on charges of wire fraud and transferring stolen identity information. Police tracked down Butler with the help of an informant from Pennsylvania who purchased more than 100 credit card records from him. SC Magazine

Full Story :

http://www.scmagazineus.com/13-years-in-prison-cometh-for-the-iceman-hacker/article/163867/?utm_source=feedbu

• Cybercriminals exploiting luger's death, Winter Olympics

Cybercriminals have been capitalizing on the world's interest in the Winter Olympics in Vancouver to spread malware, experts warned.

Attackers have been utilizing Twitter and black hat search engine (SEO) optimization tactics to promote fake Olympics' videos that are spreading malware.

Within hours after Friday's death of Georgian luge athlete, Nodar Kumaritashvili, searches for "Olympic luge crash video" were poisoned to yield a malicious link near the top of search results, Roger Thompson, chief research officer at anti-virus vendor AVG Technologies, told SCMagazineUS.com on Tuesday. Users who visited the site were told they needed to download a codec to watch the video. The codec was actually malware. SC Magazine

Full Story :

http://www.scmagazineus.com/cybercriminals-exploiting-lugers-death-winter-olympics/article/163849/?utm_source=

• Rogue antivirus program comes with tech support

IDG News Service - In an effort to boost sales, sellers of a fake antivirus product known as Live PC Care are offering their victims live technical support.

According to researchers at Symantec, once users have installed the program, they see a screen, falsely informing them that their PC is infected with several types of malware. That's typical of this type of program. What's unusual, however, is the fact that the free trial version of Live PC Care includes a big yellow "online support" button.

Clicking on the button connects the victim with an agent, who will answer questions about the product via instant message. Computerworld

Full Story :

http://www.computerworld.com/s/article/9156638/Rogue_antivirus_program_comes_with_tech_support?source=rss

New Vulnerabilities Tested in SecureScout

• 18705 Windows Kernel Exception Handler Vulnerability (MS10-015/977165) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows Kernel due to the way the kernel handles certain exceptions. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.

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

References:

- * BUGTRAQ: 20100119 Microsoft Windows NT #GP Trap Handler Allows Users to Switch Kernel Stack
<http://www.securityfocus.com/archive/1/archive/1/509106/100/0/threaded>
- * FULLDISC: 20100119 Microsoft Windows NT #GP Trap Handler Allows Users to Switch Kernel Stack

<http://seclists.org/fulldisclosure/2010/Jan/341>

* MLIST: [dailydave] 20100119 We hold these axioms to be self evident

<http://lists.immunitysec.com/pipermail/dailydave/2010-January/006000.html>

* MISC:

<http://lock.cmpxchg8b.com/c0af0967d904cef2ad4db766a00bc6af/KiTrap0D.zip>

* CONFIRM:

<http://blogs.technet.com/msrc/archive/2010/01/20/security-advisory-979682-released.aspx>

* CONFIRM:

<http://www.microsoft.com/technet/security/advisory/979682.msp>

* MS: MS10-015

<http://www.microsoft.com/technet/security/Bulletin/MS10-015.msp>

* BID: 37864

<http://www.securityfocus.com/bid/37864>

* SECTrack: 1023471

<http://securitytracker.com/id?1023471>

* SECUNIA: 38265

<http://secunia.com/advisories/38265>

* VUPEN: ADV-2010-0179

<http://www.vupen.com/english/advisories/2010/0179>

* XF: ms-win-gptrap-privilege-escalation(55742)

<http://xforce.iss.net/xforce/xfdb/55742>

CVE Reference:

CVE-2010-0232 (cve.mitre.org, nvd.nist.gov)

• 18706 Windows Kernel Double Free Vulnerability (MS10-015/977165) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows Kernel due to a double free condition. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.

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

References:

* MS: MS10-015

<http://www.microsoft.com/technet/security/Bulletin/MS10-015.msp>

* BID: 38044

<http://www.securityfocus.com/bid/38044>

* VUPEN: VUPEN/ADV-2010-0348

<http://www.vupen.com/english/advisories/2010/0348>

* SECTrack: 1023570

<http://securitytracker.com/alerts/2010/Feb/1023570.html>

CVE Reference:

CVE-2010-0233 (cve.mitre.org, nvd.nist.gov)

• 18707 PowerPoint File Path Handling Buffer Overflow Vulnerability (MS10-004/975416) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint 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: MS10-004

<http://www.microsoft.com/technet/security/Bulletin/MS10-004.msp>

* BID: 38099

<http://www.securityfocus.com/bid/38099>

* SECTrack: 1023563

<http://securitytracker.com/alerts/2010/Feb/1023563.html>

* VUPEN: VUPEN/ADV-2010-0337

<http://www.vupen.com/english/advisories/2010/0337>

CVE Reference:

CVE-2010-0029 (cve.mitre.org, nvd.nist.gov)

• **18708 PowerPoint LinkedSlideAtom Heap Overflow Vulnerability (MS10-004/975416) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint 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: MS10-004
<http://www.microsoft.com/technet/security/Bulletin/MS10-004.msp>
- * BID: 38101
<http://www.securityfocus.com/bid/38101>
- * SECTRAK: 1023563
<http://securitytracker.com/alerts/2010/Feb/1023563.html>
- * VUPEN: VUPEN/ADV-2010-0337
<http://www.vupen.com/english/advisories/2010/0337>

CVE Reference:

CVE-2010-0030 (cve.mitre.org, nvd.nist.gov)

• **18709 PowerPoint OEPlaceholderAtom 'placementId' Invalid Array Indexing Vulnerability (MS10-004/975416) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint 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: MS10-004
<http://www.microsoft.com/technet/security/Bulletin/MS10-004.msp>
- * BID: 38103
<http://www.securityfocus.com/bid/38103>
- * SECTRAK: 1023563
<http://securitytracker.com/alerts/2010/Feb/1023563.html>
- * VUPEN: VUPEN/ADV-2010-0337
<http://www.vupen.com/english/advisories/2010/0337>

CVE Reference:

CVE-2010-0031 (cve.mitre.org, nvd.nist.gov)

• **18710 PowerPoint OEPlaceholderAtom Use After Free Vulnerability (MS10-004/975416) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint 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: MS10-004
<http://www.microsoft.com/technet/security/Bulletin/MS10-004.msp>
- * BID: 38104
<http://www.securityfocus.com/bid/38104>
- * SECTRAK: 1023563
<http://securitytracker.com/alerts/2010/Feb/1023563.html>
- * VUPEN: VUPEN/ADV-2010-0337
<http://www.vupen.com/english/advisories/2010/0337>

CVE Reference:

CVE-2010-0032 (cve.mitre.org, nvd.nist.gov)

• **18711 PowerPoint Viewer TextBytesAtom Record Stack Overflow Vulnerability (MS10-004/975416) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint viewer handles specially crafted PowerPoint 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: MS10-004
<http://www.microsoft.com/technet/security/Bulletin/MS10-004.msp>
- * BID: 38107
<http://www.securityfocus.com/bid/38107>
- * SECTRAK: 1023563
<http://securitytracker.com/alerts/2010/Feb/1023563.html>
- * VUPEN: VUPEN/ADV-2010-0337
<http://www.vupen.com/english/advisories/2010/0337>

CVE Reference:

CVE-2010-0033 (cve.mitre.org, nvd.nist.gov)

• **18712 Office PowerPoint Viewer TextCharsAtom Record Stack Overflow Vulnerability (MS10-004/975416) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint Viewer handles specially crafted PowerPoint 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: MS10-004
<http://www.microsoft.com/technet/security/Bulletin/MS10-004.msp>
- * BID: 38108
<http://www.securityfocus.com/bid/38108>
- * SECTRAK: 1023563
<http://securitytracker.com/alerts/2010/Feb/1023563.html>
- * VUPEN: VUPEN/ADV-2010-0337
<http://www.vupen.com/english/advisories/2010/0337>

CVE Reference:

CVE-2010-0034 (cve.mitre.org, nvd.nist.gov)

• **18713 URL Validation Vulnerability (MS10-007/975713) (Remote File Checking)**

A remote code execution vulnerability exists in affected versions of Microsoft Windows. The vulnerability results from the incorrect validation of input sent to the ShellExecute API function. 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: 37884
<http://www.securityfocus.com/bid/37884>
- * SECTRAK: 1023495
<http://securitytracker.com/alerts/2010/Jan/1023495.html>
- * VUPEN: VUPEN/ADV-2010-0340
<http://www.vupen.com/english/advisories/2010/0340>
- * MS: MS10-007
<http://www.microsoft.com/technet/security/Bulletin/MS10-007.msp>
- * XF: ie-url-code-execution(55773)
<http://xforce.iss.net/xforce/xfdb/55773>

CVE Reference:

CVE-2010-0027 (cve.mitre.org, nvd.nist.gov)

- **18714 DirectShow Heap Overflow Vulnerability (MS10-013/977935) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft DirectShow parses AVI media files. This vulnerability could allow remote code execution if a user opened a specially crafted AVI file. If a user is logged on with administrative user rights, 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:

- * BID: 38112
<http://www.securityfocus.com/bid/38112>
- * SECTRAK: 1023562
<http://securitytracker.com/alerts/2010/Feb/1023562.html>
- * VUPEN: VUPEN/ADV-2010-0346
<http://www.vupen.com/english/advisories/2010/0346>
- * MS: MS10-013
<http://www.microsoft.com/technet/security/Bulletin/MS10-013.msp>

CVE Reference:

CVE-2010-0250 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2010-0652 Microsoft CVSS 2.0 Score = 4.3**

Microsoft Internet Explorer permits cross-origin loading of CSS stylesheets even when the stylesheet download has an incorrect MIME type and the stylesheet document is malformed, which allows remote HTTP servers to obtain sensitive information via a crafted document.

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

References:

MISC: <http://code.google.com/p/chromium/issues/detail?id=9877>

CVE Reference: [CVE-2010-0652](#)

- **CVE-2010-0108 Symantec CVSS 2.0 Score = 10.0**

Buffer overflow in the cliproxy.objects.1 ActiveX control in the Symantec Client Proxy (CLIPROXY.DLL) in Symantec AntiVirus 10.0.x, 10.1.x before MR9, and 10.2.x before MR4; and Symantec Client Security 3.0.x and 3.1.x before MR9 allows remote attackers to execute arbitrary code via a long argument to the SetRemoteComputerName function.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56355>

VUPEN: <http://www.vupen.com/english/advisories/2010/0412>

CONFIRM:
http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/38222>

SECUNIA: <http://secunia.com/advisories/38651>

CVE Reference: [CVE-2010-0108](#)

- **CVE-2010-0149 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in Cisco ASA 5500 Series Adaptive Security Appliance 7.2 before 7.2(4.46), 8.0 before 8.0(4.38), 8.1 before 8.1(2.29), and 8.2 before 8.2(1.5); and Cisco PIX 500 Series Security Appliance; allows remote attackers to cause a denial of service (prevention of new connections) via crafted TCP segments during termination of the TCP connection that cause the connection to remain in CLOSEWAIT status, aka "TCP Connection Exhaustion"

Denial of Service Vulnerability."

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56336>

VUPEN: <http://www.vupen.com/english/advisories/2010/0415>

SECTRAK: <http://www.securitytracker.com/id?1023612>

BID: <http://www.securityfocus.com/bid/38275>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1910c.shtml

SECUNIA: <http://secunia.com/advisories/38636>

SECUNIA: <http://secunia.com/advisories/38618>

OSVDB: <http://osvdb.org/62433>

CVE Reference: [CVE-2010-0149](#)

• **CVE-2010-0150 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in Cisco ASA 5500 Series Adaptive Security Appliance 7.0 before 7.0(8.10), 7.2 before 7.2(4.45), 8.0 before 8.0(5.2), 8.1 before 8.1(2.37), and 8.2 before 8.2(1.16); and Cisco PIX 500 Series Security Appliance; allows remote attackers to cause a denial of service (device reload) via malformed SIP messages, aka Bug ID CSCsy91157.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56338>

VUPEN: <http://www.vupen.com/english/advisories/2010/0415>

SECTRAK: <http://www.securitytracker.com/id?1023612>

BID: <http://www.securityfocus.com/bid/38277>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1910c.shtml

SECUNIA: <http://secunia.com/advisories/38636>

SECUNIA: <http://secunia.com/advisories/38618>

OSVDB: <http://osvdb.org/62434>

CVE Reference: [CVE-2010-0150](#)

• **CVE-2010-0151 Cisco CVSS 2.0 Score = 7.8**

The Cisco Firewall Services Module (FWSM) 4.0 before 4.0(8), as used in for the Cisco Catalyst 6500 switches, Cisco 7600 routers, and ASA 5500 Adaptive Security Appliances, allows remote attackers to cause a denial of service (crash) via a malformed Skinny Client Control Protocol (SCCP) message.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1910e.shtml

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1910c.shtml

XF: <http://xforce.iss.net/xforce/xfdb/56333>

VUPEN: <http://www.vupen.com/english/advisories/2010/0418>

SECTRAK: <http://www.securitytracker.com/id?1023609>

BID: <http://www.securityfocus.com/bid/38274>

SECUNIA: <http://secunia.com/advisories/38621>

OSVDB: <http://osvdb.org/62432>

CVE Reference: [CVE-2010-0151](#)

• **CVE-2010-0565 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in Cisco ASA 5500 Series Adaptive Security Appliance 7.2 before 7.2(4.45), 8.0 before 8.0(4.44), 8.1 before 8.1(2.35), and 8.2 before 8.2(1.10), allows remote attackers to cause a denial of service (page fault and device reload) via a malformed DTLS message, aka Bug ID CSCtb64913 and "WebVPN DTLS Denial of Service Vulnerability."

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56339>

VUPEN: <http://www.vupen.com/english/advisories/2010/0415>

SECTRAK: <http://www.securitytracker.com/id?1023612>

BID: <http://www.securityfocus.com/bid/38280>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1910c.shtml

SECUNIA: <http://secunia.com/advisories/38618>

OSVDB: <http://osvdb.org/62430>

CVE Reference: [CVE-2010-0565](#)

• **CVE-2010-0569 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in Cisco ASA 5500 Series Adaptive Security Appliance 7.0 before 7.0(8.10), 7.2 before 7.2(4.45), 8.0 before 8.0(5.2), 8.1 before 8.1(2.37), and 8.2 before 8.2(1.16); and Cisco PIX 500 Series Security Appliance; allows remote attackers to cause a denial of service (device reload) via malformed SIP messages, aka Bug ID CSCtc96018.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56337>

VUPEN: <http://www.vupen.com/english/advisories/2010/0415>

SECTRAK: <http://www.securitytracker.com/id?1023612>

BID: <http://www.securityfocus.com/bid/38281>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1910c.shtml

SECUNIA: <http://secunia.com/advisories/38636>

SECUNIA: <http://secunia.com/advisories/38618>

OSVDB: <http://osvdb.org/62435>

CVE Reference: [CVE-2010-0569](#)

• **CVE-2010-0566 Cisco CVSS 2.0 Score = 7.1**

Unspecified vulnerability in Cisco ASA 5500 Series Adaptive Security Appliance 7.0 before 7.0(8.10), 7.2 before 7.2(4.45), 8.0 before 8.0(4.44), 8.1 before 8.1(2.35), and 8.2 before 8.2(1.10) allows remote attackers to cause a denial of service (device reload) via a malformed TCP segment when certain NAT translation and Cisco AIP-SSM configurations are used, aka Bug ID CSCtb37219.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/56340>

VUPEN: <http://www.vupen.com/english/advisories/2010/0415>

SECTRAK: <http://www.securitytracker.com/id?1023612>

BID: <http://www.securityfocus.com/bid/38278>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b1910c.shtml

SECUNIA: <http://secunia.com/advisories/38618>

OSVDB: <http://osvdb.org/62431>

CVE Reference: [CVE-2010-0566](#)

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