

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

[Winny \(WinNY\) software Scanner](#) - The S4 Winny Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if the peer-to-peer software Winny is installed and running.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winnyscanner>

This Week in Review

Trying to predict the future. SSL possible to hack. Gaza conflict also online. A recipe for securing Vista.

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

• Opinion: Security predictions for 2009

December 30, 2008 (Network World) My predictions for information security in 2009 are just predictions, not recommendations. I am trying to guess what will happen, not suggesting what should happen. As always, take these with a grain of salt.

Host-based security will become the focus for 2009. The imminent release of Windows 7 and the continued interest in Mac OS and Linux as alternative desktops are once again focusing attention on operating system and endpoint security.

Encryption will grow in use. At-rest encryption of hard drives on all desktop systems will become the norm. Servers will still lag behind. Encryption of mobile-device storage will start getting interesting. And once again in 2009, it'll still be impossible to send an encrypted e-mail to someone without making special arrangements in advance. Public-key infrastructure (PKI) encryption remains fragmented in small disconnected islands. Ugh.

Computerworld

Full Story :

• Hackers find hole to create rogue digital certificates

Researchers on Tuesday demonstrated an attack that allowed them to successfully create a rogue Certification Authority (CA) certificate, which would be trusted by all web browsers and allow an attacker to impersonate any website, including those secured by the HTTPS protocol.

Jacob Appelbaum and Alexander Sotirov presented the research at the 25th Chaos Communication Congress in Berlin during a presentation called "MD5 considered harmful today."

The research team was comprised of Sotirov, Appelbaum and David Molnar of the United States; Marc Stevens and Benne de Weger of the Netherlands; and Dag Arne Osvik and Arjen Lenstra of Switzerland.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Hackers-find-hole-to-create-rogue-digital-certificates/article/123407/>

• With Gaza conflict, cyberattacks come too

December 31, 2008 (IDG News Service) The conflict raging in Gaza between Israel and Palestine has spilled over to the Internet.

The defacements have primarily affected small businesses and vanity Web pages hosted on Israel's .il Internet domain space. One such site, Rosh Ha'ayin, Israel's Galoz Electronics Ltd, whose hacked Web site read "RitualistaS GrouP Hacked your System!!! The world isn't insurance!!! For a better world," on Wednesday.

On Saturday, Israel launched air strikes into Gaza in response to earlier rocket attacks from Hamas and other militant groups. The online attacks began soon after, Warner said. "It really got serious on Sunday," he said. "All the stops got pulled out."

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124658&source=rss> topic1

• How to secure your Vista PC in 10 easy steps

December 31, 2008 (PC World) While Windows Vista may be Microsoft Corp.'s most secure operating system ever, it's far from completely secure. In its fresh-from-the-box configuration, Vista still leaves a chance for your personal data to leak out to the Web through Windows Firewall or for some nefarious bot to tweak your browser settings without your knowledge.

1. Use Windows Security Center as a starting point For a quick overview of your security settings, the Windows Security Center is where you'll find the status of your system firewall, auto update, malware protection and other security settings. Click Start, Control Panel, Security Center, or you can simply click the shield icon in the task tray. If you see any red or yellow, you are not fully protected.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124567&source=rss> topic1

New Vulnerabilities Tested in SecureScout

• 18194 Vulnerability in Cisco IOS While Processing SSL Packet (cisco-sa-20080924-ssl)

This vulnerability is triggered during the termination of an SSL session. Possession of valid credentials such as a username, password or a certificate is not required. SSL protocol uses TCP as a transport protocol. The requirement of the complete TCP 3-way handshake reduces the probability that this vulnerability will be exploited through the use of spoofed IP addresses.

A device running vulnerable Cisco IOS Software with SSL-based service configured will crash while terminating an SSL session.

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

References:

* CISCO: 20080924 Vulnerability in Cisco IOS While Processing SSL Packet
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a0146c.shtml

CVE Reference:

CVE-2008-3798 (cve.mitre.org, nvd.nist.gov)

• 18201 Cisco IOS Software Firewall Application Inspection Control Vulnerability (cisco-sa-20080924-iosfw)

Firewalls are networking devices that control access to an organization's network assets. Firewalls are often positioned at the entrance points into networks. Cisco IOS software provides a set of security features that enable you to configure a simple or elaborate firewall policy, according to your particular requirements.

HTTP uses port 80 by default to transport Internet web services, which are commonly used on the network and rarely challenged with regard to their legitimacy and conformance to standards. Because port 80 traffic is typically allowed through the network without being challenged, many application developers are leveraging HTTP traffic as an alternative transport protocol that will allow their application's traffic to travel through or even bypass the firewall. When the Cisco IOS Firewall is configured with HTTP AIC, it performs packet inspection to detect HTTP connections that are not authorized in the scope of the security policy configuration. It also detects users who are tunneling applications through port 80. If the packet is not in compliance with the HTTP protocol, it will be dropped, the connection will be reset, and a syslog message will be generated, as appropriate.

Cisco IOS Software that is configured for IOS firewall AIC with an HTTP application-specific policy is vulnerable to a denial of service condition when it processes a specific malformed HTTP transit packet. Successful exploitation of the vulnerability may result in a reload of the affected device.

HTTP runs over TCP. For this vulnerability to be exploited, a full three-way handshake between client and server is required before any malicious traffic would be processed to result in a device reload.

Additional information regarding Cisco IOS Firewall AIC with HTTP application-specific policy maps is available at [/en/US/products/ps6441/products_feature_guide09186a008060f6dd.html#wp1407906](http://en/US/products/ps6441/products_feature_guide09186a008060f6dd.html#wp1407906).

This vulnerability is documented in Cisco bug ID CSCsh12480.

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

References:

* CONFIRM:
<http://tools.cisco.com/security/center/viewAlert.x?alertId=16661>
* CISCO: 20080924 Cisco IOS Software Firewall Application Inspection Control Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a01545.shtml

CVE Reference:

CVE-2008-3812 (cve.mitre.org, nvd.nist.gov)

• 18202 Cisco IOS Software Layer 2 Tunneling Protocol (L2TP) Denial of Service Vulnerability (cisco-sa-20080924-l2tp)

Documented in RFC2661, L2TP and RFC3931, L2TPv3 are protocols for tunneling network traffic between two peers over an existing network.

A device running affected 12.2 and 12.4 versions of Cisco IOS and that has the L2TP mgmt daemon process running will reload when processing a specially crafted L2TP packet.

Several features leverage the L2TP protocol and start the L2TP mgmt daemon within Cisco IOS. These features have been outlined in this advisory under the Vulnerable Products section.

This vulnerability is documented in Cisco bug ID CSCsh48879.

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

References:

* CISCO: 20080924 Cisco IOS Software Layer 2 Tunneling Protocol (L2TP) Denial of Service Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a0157a.shtml

CVE Reference:

CVE-2008-3813 (cve.mitre.org, nvd.nist.gov)

• 18203 PHP Buffer overflow in the imageloadfont function

Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.

The issue has been solved in PHP version 4.4.9, and 5.2.7.

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

References:

- * MISC:
<http://news.php.net/php.cvs/51219>
- * CONFIRM:
http://bugs.gentoo.org/show_bug.cgi?id=234102
- * CONFIRM:
<http://www.php.net/archive/2008.php#id2008-08-07-1>
- * MLIST: [oss-security] 20080808 CVE request: php-5.2.6 overflow issues
<http://www.openwall.com/lists/oss-security/2008/08/08/2>
- * MLIST: [oss-security] 20080813 Re: CVE request: php-5.2.6 overflow issues
<http://www.openwall.com/lists/oss-security/2008/08/13/8>
- * DEBIAN: DSA-1647
<http://www.debian.org/security/2008/dsa-1647>
- * SUSE: SUSE-SR:2008:018
<http://lists.opensuse.org/opensuse-security-announce/2008-09/msg00004.html>
- * SUSE: SUSE-SR:2008:021
<http://lists.opensuse.org/opensuse-security-announce/2008-10/msg00006.html>
- * BID: 30649
<http://www.securityfocus.com/bid/30649>
- * SECUNIA: 32148
<http://secunia.com/advisories/32148>
- * SECUNIA: 32316
<http://secunia.com/advisories/32316>

CVE Reference:

CVE-2008-3658 (cve.mitre.org, nvd.nist.gov)

• 18204 PHP `php_sprintf_appendstring()` remote Integer Overflow Vulnerability

Integer overflow in PHP 5.2.5 and earlier allows context-dependent attackers to cause a denial of service and possibly have unspecified other impact via a `printf` format parameter with a large width specifier, related to the `php_sprintf_appendstring` function in `formatted_print.c` and probably other functions for formatted strings (aka `*printf` functions).

The issue has been solved in PHP version 5.2.5.

Test Case Impact: **Attack** Vulnerability Impact: **DoS / Attack** Risk: **Medium**

References:

- * SREASONRES: 20080320 PHP 5.2.5 and prior : `*printf()` functions Integer Overflow
http://securityreason.com/achievement_securityalert/52
- * BUGTRAQ: 20080321 {securityreason.com}PHP 5 `*printf()` - Integer Overflow
<http://www.securityfocus.com/archive/1/archive/1/489962/100/0/threaded>
- * BUGTRAQ: 20080523 rPSA-2008-0176-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl
<http://www.securityfocus.com/archive/1/archive/1/492535/100/0/threaded>
- * BUGTRAQ: 20080527 rPSA-2008-0178-1 php php-mysql php-pgsql
<http://www.securityfocus.com/archive/1/archive/1/492671/100/0/threaded>
- * CONFIRM:
<http://cvs.php.net/viewvc.cgi/php-src/NEWS?revision=1.2027.2.547.2.1120&view=markup>
- * CONFIRM:
<http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0176>
- * CONFIRM:
<https://issues.rpath.com/browse/RPL-2503>
- * CONFIRM:
<http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0178>
- * SUSE: SUSE-SR:2008:014
<http://lists.opensuse.org/opensuse-security-announce/2008-07/msg00001.html>
- * UBUNTU: USN-628-1
<http://www.ubuntu.com/usn/usn-628-1>

* BID: 28392
<http://www.securityfocus.com/bid/28392>
* SECUNIA: 30345
<http://secunia.com/advisories/30345>
* SECUNIA: 30411
<http://secunia.com/advisories/30411>
* SECUNIA: 30967
<http://secunia.com/advisories/30967>
* SECUNIA: 31200
<http://secunia.com/advisories/31200>
* XF: php-phpsprintfappendstring-overflow(41386)
<http://xforce.iss.net/xforce/xfdb/41386>

CVE Reference:

CVE-2008-1384 (cve.mitre.org, nvd.nist.gov)

• **18206 Vulnerability in Server Service Could Allow Remote Code Execution (MS06-040/921883) (Network Check)**

There is a remote code execution vulnerability in Server Service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:

* CISCO: 20060814 Mitigating Exploitation of the MS06-040 Service Buffer Vulnerability
http://www.cisco.com/en/US/products/ps6120/tsd_products_security_response09186a008070c75a.html
* MS: MS06-040
<http://www.microsoft.com/technet/security/bulletin/ms06-040.msp>
* CERT: TA06-220A
<http://www.us-cert.gov/cas/techalerts/TA06-220A.html>
* CERT-VN: VU#650769
<http://www.kb.cert.org/vuls/id/650769>
* BID: 19409
<http://www.securityfocus.com/bid/19409>
* FRSIRT: ADV-2006-3210
<http://www.frsirt.com/english/advisories/2006/3210>
* OVAL: oval:org.mitre.oval:def:492
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:492>
* SECTRAK: 1016667
<http://securitytracker.com/id?1016667>
* SECUNIA: 21388
<http://secunia.com/advisories/21388>
* XF: ms-server-service-bo(28002)
<http://xforce.iss.net/xforce/xfdb/28002>

CVE Reference:

CVE-2006-3439 (cve.mitre.org, nvd.nist.gov)

• **18207 Server Service Vulnerability (MS08-067/958644) (Network Check)**

A remote code execution vulnerability exists in the Server service on Windows systems. The vulnerability is due to the service not properly handling specially crafted RPC requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Test Case Impact: **Denial of Service** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: MS08-067
<http://www.microsoft.com/technet/security/Bulletin/ms08-067.msp>
* CERT-VN: VU#827267
<http://www.kb.cert.org/vuls/id/827267>
* FRSIRT: ADV-2008-2902
<http://www.frsirt.com/english/advisories/2008/2902>
* SECUNIA: 32326
<http://secunia.com/advisories/32326>
* XF: win-server-rpc-code-execution(46040)
<http://xforce.iss.net/xforce/xfdb/46040>

CVE Reference:

CVE-2008-4250 (cve.mitre.org, nvd.nist.gov)

• **18215 Oracle Application Server - Oracle Portal component unspecified Vulnerability (oct-2008/CVE-2008-3975)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Portal" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>
- * FRSIRT: ADV-2008-2825
<http://www.frsirt.com/english/advisories/2008/2825>
- * SECTrack: 1021054
<http://www.securitytracker.com/id?1021054>
- * SECUNIA: 32291
<http://secunia.com/advisories/32291>
- * XF: oracle-appserver-portaltools-unspecified1(45881)
<http://xforce.iss.net/xforce/xfdb/45881>

CVE Reference:

CVE-2008-3975 (cve.mitre.org, nvd.nist.gov)

• **18216 Oracle Application Server - Oracle Portal component unspecified Vulnerability (oct-2008/CVE-2008-3977)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Portal" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>
- * FRSIRT: ADV-2008-2825
<http://www.frsirt.com/english/advisories/2008/2825>
- * SECTrack: 1021054
<http://www.securitytracker.com/id?1021054>
- * SECUNIA: 32291
<http://secunia.com/advisories/32291>

CVE Reference:

CVE-2008-3977 (cve.mitre.org, nvd.nist.gov)

• **18249 Internet Explorer Pointer Reference Memory Corruption Vulnerability (MS08-078/960714) (Remote File Checking)**

A remote code execution vulnerability exists as an invalid pointer reference in the data binding function of Internet Explorer. When data binding is enabled (which is the default state), it is possible under certain conditions for an object to be released without updating the array length, leaving the potential to access the deleted object's memory space. This can cause Internet Explorer to exit unexpectedly, in a state that is exploitable.

An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.

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

References:

- * MILWORM: 7403
<http://www.milw0rm.com/exploits/7403>
- * MILWORM: 7410
<http://www.milw0rm.com/exploits/7410>
- * MILWORM: 7477
<http://www.milw0rm.com/exploits/7477>
- * MISC:
<http://isc.sans.org/diary.html?storyid=5458>
- * MISC:
<http://www.avertlabs.com/research/blog/index.php/2008/12/09/yet-another-unpatched-drive-by-exploit-found-on-the-web/>
- * MISC:

<http://www.breakingpointsystems.com/community/blog/patch-tuesdays-and-drive-by-sundays>

* MISC:

<http://www.scanw.com/blog/archives/303>

* CONFIRM:

<http://www.microsoft.com/technet/security/advisory/961051.msp>

* CERT-VN: VU#493881

<http://www.kb.cert.org/vuls/id/493881>

* BID: 32721

<http://www.securityfocus.com/bid/32721>

* SECUNIA: 33089

<http://secunia.com/advisories/33089>

CVE Reference:

CVE-2008-4844 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-5745 Microsoft CVSS 2.0 Score = 9.3

Integer overflow in Microsoft Windows Media Player 9, 10, and 11 allows remote attackers to execute arbitrary code via a crafted (1) WAV, (2) SND, or (3) MID file. NOTE: it is not clear whether this vulnerability is related to CVE-2008-4927 or CVE-2008-2253.

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

References:

SECTRAK: <http://www.securitytracker.com/id?1021495>

BID: <http://www.securityfocus.com/bid/33018>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/499579/100/0/threaded>

CVE Reference: [CVE-2008-5745](#)

• CVE-2008-5750 Microsoft CVSS 2.0 Score = 6.8

Argument injection vulnerability in Microsoft Internet Explorer 8 beta 2 on Windows XP SP3 allows remote attackers to execute arbitrary commands via the --renderer-path option in a chromehtml: URI.

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

References:

BID: <http://www.securityfocus.com/bid/32999>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/499570/100/0/threaded>

MILWORM: <http://www.milw0rm.com/exploits/7566>

MISC: http://retrogod.altervista.org/9sg_chrome.html

CVE Reference: [CVE-2008-5750](#)

• CVE-2008-5746 Sun CVSS 2.0 Score = 6.9

Sun SNMP Management Agent (SUNWmasf) 1.4u2 through 1.5.4 allows local users to overwrite arbitrary files and gain privileges via a symlink attack on temporary files.<http://sunsolve.sun.com/search/document.do?assetkey=1-26-248646-1> This issue can occur in the following releases: SPARC Platform * Sun SNMP Management Agent "SUNWmasf" 1.4u2 thru 1.5.4 (For Solaris 8, 9 and 10)

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

References:

SECTRAK: <http://www.securitytracker.com/id?1021496>

BID: <http://www.securityfocus.com/bid/33014>

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-248646-1>

SECUNIA: <http://secunia.com/advisories/33328>

CVE Reference: [CVE-2008-5746](#)

• **CVE-2008-5747 F-Prot CVSS 2.0 Score = 5.0**

F-Prot 4.6.8 for GNU/Linux allows remote attackers to bypass anti-virus protection via a crafted ELF program with a "corrupted" header that still allows the program to be executed. NOTE: due to an error in the initial disclosure, F-secure was incorrectly stated as the vendor.

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

References:

BID: <http://www.securityfocus.com/bid/32753>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/499501/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/499305/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/499083>

MISC: <http://www.ivizsecurity.com/security-advisory-iviz-sr-08016.html>

CVE Reference: [CVE-2008-5747](#)

• **CVE-2008-5749 Google CVSS 2.0 Score = 6.8**

**** DISPUTED **** Argument injection vulnerability in Google Chrome 1.0.154.36 on Windows XP SP3 allows remote attackers to execute arbitrary commands via the --renderer-path option in a chromehtml: URI. NOTE: a third party disputes this issue, stating that Chrome "will ask for user permission" and "cannot launch the applet even [if] you have given out the permission."

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

References:

BID: <http://www.securityfocus.com/bid/32997>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/499581/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/499570/100/0/threaded>

MILWORM: <http://www.milw0rm.com/exploits/7566>

MISC: http://retrogod.altervista.org/9sq_chrome.html

CVE Reference: [CVE-2008-5749](#)

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