

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.

CTO Jesper Jurcenoks of netVigilance is the keynote speaker at the ITEC Conference & Exhibition 2008 in Dallas June 4-5, see

<http://www.netvigilance.com/events>

This Week in Review

A tool that keeps track of botnets. HIPAA in need of better oversight. A simpler way to quantum cryptography makes it cheaper. Security in a world of free information flow.

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

❖ Microsoft botnet-hunting tool helps bust hackers

Super-secret tool not even to be named in public

Botnet fighters have another tool in their arsenal, thanks to Microsoft Corp.

The software vendor is giving law enforcers access to a special tool that keeps tabs on botnets, using data compiled from the 450 million computer users who have installed the Malicious Software Removal Tool that ships with Windows.

Although Microsoft is reluctant to give out details on its botnet buster -- the company said that even revealing its name could give cybercriminals a clue on how to thwart it -- company executives discussed it at a closed-door conference held for law enforcement professionals Monday.

computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9080958&source=rss_topic85

❖ Proliferating HIPAA complaints and medical record breaches

The number of complaints regarding violations of the U.S. Health Insurance Portability and Accountability Act (HIPAA) continue to increase each year in tandem with an increase in breaches of medical records, according to one security professional.

In addition, a growing number of these complaints are going unresolved.

The protected health information (PHI) security and privacy goals of HIPAA in spirit and intent are good, Herold, leader of the Realtime IT Compliance Community, told SCMagazineUS.com on Friday. The regulatory oversight of the U.S. Department of Health and Human Services (HSS), however, has been underwhelming, she said.

scmagazine

Full Story :

<http://www.scmagazineus.com/Proliferating-HIPAA-complaints-and-medical-record-breaches/article/110555/>

❖ Researchers Look to Cut Quantum Cryptography Costs

Researchers at the National Institute of Standards and Technology want cut the cost of quantum cryptography.

A team of researchers at the National Institute of Standards and Technology is touting a new method of cutting the costs associated with quantum key distribution. In a soon-to-be-published paper, researchers at NIST outline a technique that simplifies the structure of a QKD system, slashing its costs by reducing the number of single photon detectors it needs.

eweek

Full Story :

<http://www.eweek.com/c/a/Security/Researchers-Look-to-Cut-Quantum-Cryptography-Costs/>

❖ **Opinion: Better than locks: A security approach to "free"**

Keeping security relevant in the free-content era

In January, Kevin Kelly wrote an essay entitled "Better Than Free" that explained which concepts held value on the Internet. This generated a lot of interest, mostly around the question of how best to make money out of these concepts. As a career security guy, I found myself wondering how on earth my field will respond -- how does security need to adapt to support business models based on these values? When we're used to locking everything down, how do we respond when people start calling for openness?

Kelly's essay set out one of those ideas that sound completely obvious once you've heard them: When something that can be copied comes into contact with the Internet, copies soon become freely available.

computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9084988&taxonomyId=17&intsrc=kc_feat

New Vulnerabilities Tested in SecureScout

❖ **14060 Samba stack-based buffer overflow in the send_mailslot function Vulnerability**

Stack-based buffer overflow in the send_mailslot function in nmbd in Samba, when the "domain logons" option is enabled, allows remote attackers to execute arbitrary code via a GETDC mailslot request composed of a long GETDC string following an offset username in a SAMLOGON logon request.

The security issue has been fixed in version 3.0.27a.

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

Some references:

* BUGTRAQ: 20071210 Secunia Research: Samba "send_mailslot()" Buffer Overflow Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/484818/100/0/threaded>

* BUGTRAQ: 20071210 [SECURITY] Buffer overrun in send_mailslot()

<http://www.securityfocus.com/archive/1/archive/1/484825/100/0/threaded>

* BUGTRAQ: 20071210 rPSA-2007-0261-1 samba samba-swat

<http://www.securityfocus.com/archive/1/archive/1/484827/100/0/threaded>

* BUGTRAQ: 20071214 POC for samba send_mailslot()

<http://www.securityfocus.com/archive/1/archive/1/485144/100/0/threaded>

* BUGTRAQ: 20080221 VMSA-2008-0003 Moderate: Updated aacraid driver and samba and python service console updates

<http://www.securityfocus.com/archive/1/archive/1/488457/100/0/threaded>

* MLIST: [Security-announce] 20080221 VMSA-2008-0003 Moderate: Updated aacraid driver and samba and python service console updates

<http://lists.vmware.com/pipermail/security-announce/2008/000005.html>

* MISC:

http://secunia.com/secunia_research/2007-99/advisory/

* CONFIRM:

<http://www.samba.org/samba/security/CVE-2007-6015.html>

* CONFIRM:

http://bugs.gentoo.org/show_bug.cgi?id=200773

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2007-520.htm>

CVE Reference: [CVE-2007-6015](#)

❖ **14061 Samba "receive_smb_raw()" Buffer Overflow Vulnerability**

Secunia Research has discovered a vulnerability in Samba, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the "receive_smb_raw()" function in lib/util_sock.c when parsing SMB packets. This can be exploited to cause a heap-based buffer overflow via an overly large SMB packet received in a client context.

Successful exploitation allows execution of arbitrary code by tricking a user into connecting to a malicious server (e.g. by clicking an "smb://" link) or by sending specially crafted packets to an "nmbd" server configured as a local or domain master browser.

Samba version 3.0.30 fixes the issue.

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

References:

* SECUNIA: 30228

<http://secunia.com/advisories/30228/>

* SECUNIA: Samba "receive_smb_raw()" Buffer Overflow Vulnerability

http://secunia.com/secunia_research/2008-20/advisory/

* MISC:

<http://www.securityfocus.com/archive/1/492683>

CVE Reference: [CVE-2008-1105](#)

❖ **16935 OpenSSL Server Name extension crash Vulnerability**

Testing using the Codenomicon TLS test suite discovered a flaw in the handling of server name extension data in OpenSSL 0.9.8f and OpenSSL 0.9.8g. If OpenSSL has been compiled using the non-default TLS server name extensions, a remote attacker could send a carefully crafted packet to a server application using OpenSSL and cause it to crash. (CVE-2008-0891).

Please note this issue does not affect any other released versions of OpenSSL, and does not affect versions compiled without TLS server name extensions.

Users of OpenSSL 0.9.8f or 0.9.8g should update to the OpenSSL 0.9.8h release which contains a patch to correct this issue.

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

References:

- * CONFIRM:
http://www.openssl.org/news/secadv_20080528.txt
- * SECUNIA: 30405
<http://secunia.com/advisories/30405/>
- * BID: 29405
<http://www.securityfocus.com/bid/29405>
- * SECTrack: 1020121
<http://www.securitytracker.com/alerts/2008/May/1020121.html>
- * FRsIRT: FRsIRT/ADV-2008-1680
<http://www.frsirt.com/english/advisories/2008/1680>

CVE Reference: [CVE-2008-0891](#)

❖ **16936 OpenSSL Omit Server Key Exchange message crash Vulnerability**

Testing using the Codenomicon TLS test suite discovered a flaw if the 'Server Key exchange message' is omitted from a TLS handshake in OpenSSL 0.9.8f and OpenSSL 0.9.8g. If a client connects to a malicious server with particular cipher suites, the server could cause the client to crash. (CVE-2008-1672).

Please note this issue does not affect any other released versions of OpenSSL.

Users of OpenSSL 0.9.8f or 0.9.8g should update to the OpenSSL 0.9.8h release which contains a patch to correct this issue.

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

References:

- * CONFIRM:
http://www.openssl.org/news/secadv_20080528.txt
- * SECUNIA: 30405
<http://secunia.com/advisories/30405/>
- * BID: 29405
<http://www.securityfocus.com/bid/29405>
- * SECTrack: 1020122
<http://www.securitytracker.com/alerts/2008/May/1020122.html>
- * FRsIRT: FRsIRT/ADV-2008-1680
<http://www.frsirt.com/english/advisories/2008/1680>

CVE Reference: [CVE-2008-1672](#)

❖ **16937 Trillian X-MMS-IM-FORMAT header in an MSN message arbitrary**

code execution Vulnerability (Remote File Checking)

Stack-based buffer overflow in Cerulean Studios Trillian allows remote attackers to execute arbitrary code via unspecified attributes in the X-MMS-IM-FORMAT header in an MSN message.

The vulnerability is reported fixed in version 3.1.10.0.

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

References:

- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-031/>
- * BUGTRAQ: 20080521 ZDI-08-031: Trillian MSN MIME Header Stack-Based Overflow Vulnerability
<http://archives.neohapsis.com/archives/bugtraq/2008-05/0285.html>
- * XF: trillian-msn-protocol-bo(42576)
<http://xforce.iss.net/xforce/xfdb/42576>
- * BID: 29330
<http://www.securityfocus.com/bid/29330>
- * FRSIRT: ADV-2008-1622
<http://www.frsirt.com/english/advisories/2008/1622>
- * SECTRAK: 1020106
<http://securitytracker.com/id?1020106>
- * SECUNIA: 30336
<http://secunia.com/advisories/30336>

CVE Reference: [CVE-2008-2409](#)

❖ 16938 Trillian XML parsing functionality arbitrary code execution Vulnerability (Remote File Checking)

Heap-based buffer overflow in the XML parsing functionality in talk.dll in Cerulean Studios Trillian Pro allows remote attackers to execute arbitrary code via a malformed attribute in an IMG tag.

The vulnerability is reported fixed in version 3.1.10.0.

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

References:

- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-030/>
- * BUGTRAQ: 20080521 ZDI-08-030: Trillian Multiple Protocol XML Parsing Memory Corruption Vulnerability
<http://archives.neohapsis.com/archives/bugtraq/2008-05/0284.html>
- * XF: trillian-talk-bo(42581)
<http://xforce.iss.net/xforce/xfdb/42581>
- * BID: 29330

<http://www.securityfocus.com/bid/29330>

* FRSIRT: ADV-2008-1622

<http://www.frsirt.com/english/advisories/2008/1622>

* SECTrack: 1020105

<http://securitytracker.com/id?1020105>

* SECUNIA: 30336

<http://secunia.com/advisories/30336>

CVE Reference: [CVE-2008-2408](#)

❖ **16939 Trillian stack-based buffer overflow in AIM.DLL arbitrary code execution Vulnerability (Remote File Checking)**

Stack-based buffer overflow in AIM.DLL in Cerulean Studios Trillian allows user-assisted remote attackers to execute arbitrary code via a long attribute value in a FONT tag in a message.

The vulnerability is reported fixed in version 3.1.10.0.

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

References:

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-029/>

* BUGTRAQ: 20080521 ZDI-08-029: Trillian AIM.DLL Long HTML Font Parameter Stack Overflow Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/492433/100/0/threaded>

* XF: trillian-aimdll-bo(42582)

<http://xforce.iss.net/xforce/xfdb/42582>

* BID: 29330

<http://www.securityfocus.com/bid/29330>

* FRSIRT: ADV-2008-1622

<http://www.frsirt.com/english/advisories/2008/1622>

* SECTrack: 1020104

<http://securitytracker.com/id?1020104>

* SECUNIA: 30336

<http://secunia.com/advisories/30336>

CVE Reference: [CVE-2008-2407](#)

❖ **16940 Trillian Display Names message feature arbitrary code execution and Denial of Service Vulnerability (Remote File Checking)**

Buffer overflow in the Display Names message feature in Cerulean Studios Trillian allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long nickname in an MSN protocol message.

The vulnerability is reported fixed in version 3.1.10.0.

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

References:

- * BUGTRAQ: 20080424 Trillian 3.1 basic nick crash
<http://www.securityfocus.com/archive/1/archive/1/491281/100/0/threaded>
- * BID: 28925
<http://www.securityfocus.com/bid/28925>
- * FRSIRT: ADV-2008-1368
<http://www.frsirt.com/english/advisories/2008/1368/references>
- * SECUNIA: 29952
<http://secunia.com/advisories/29952>

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

❖ **16941 Trillian malformed aim: URI buffer overflow Vulnerability (Remote File Checking)**

Buffer overflow in the AOL Instant Messenger (AIM) protocol handler in AIM.DLL in Cerulean Studios Trillian allows remote attackers to execute arbitrary code via a malformed aim: URI, as demonstrated by a long URI beginning with the aim:///#1111111/ substring.

The vulnerability is reported fixed in version 3.1.7.0.

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

References:

- * FULLDISC: 20070718 Can CERT VU#786920 be right?
<http://archives.neohapsis.com/archives/fulldisclosure/2007-07/0356.html>
- * MISC:
<http://www.xs-sniper.com/nmcfeters/Cross-App-Scripting-2.html>
- * CERT-VN: VU#786920
<http://www.kb.cert.org/vuls/id/786920>
- * BID: 24927
<http://www.securityfocus.com/bid/24927>
- * FRSIRT: ADV-2007-2546
<http://www.frsirt.com/english/advisories/2007/2546>
- * SECUNIA: 26086
<http://secunia.com/advisories/26086>
- * XF: trillian-aim-bo(35447)
<http://xforce.iss.net/xforce/xfdb/35447>

Product Homepage:

<http://www.wireshark.org/>

CVE Reference: [CVE-2007-3832](#)

❖ **16942 Trillian "aim: &c:\\" URI file creation with arbitrary content Vulnerability (Remote File Checking)**

The AOL Instant Messenger (AIM) protocol handler in Cerulean Studios Trillian allows remote attackers to create files with arbitrary contents via certain aim: URIs, as

demonstrated by a URI that begins with the "aim: &c:\" substring and contains a full pathname in the ini field. NOTE: this can be leveraged for code execution by writing to a Startup folder.

The vulnerability is reported fixed in version 3.1.7.0.

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

References:

- * MISC:
<http://www.xs-sniper.com/nmcfeters/Cross-App-Scripting-2.html>
- * BID: 24927
<http://www.securityfocus.com/bid/24927>
- * FRSIRT: ADV-2007-2546
<http://www.frsirt.com/english/advisories/2007/2546>
- * SECUNIA: 26086
<http://secunia.com/advisories/26086>
- * XF: trillian-aim-file-create(35449)
<http://xforce.iss.net/xforce/xfdb/35449>

CVE Reference: [CVE-2007-3833](#)

New Vulnerabilities found this Week

Adobe Flash Player Unspecified Vulnerability

“Compromise a user's system”

A vulnerability has been reported in Adobe Flash Player, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error. No further information is currently available. Reportedly, this is currently being actively exploited.

The vulnerability is reported in version 9.0.124.0. Other versions may also be affected.

References:

- http://blogs.adobe.com/psirt/2008/05/potential_flash_player_issue.html
- <http://isc.sans.org/diary.html?storyid=4465>

OpenSSL Two Denial of Service Vulnerabilities

“Denial of Service”

Two vulnerabilities have been reported in OpenSSL, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) A double-free error in the handling of server name extension data can be exploited to crash a server application using OpenSSL.

Successful exploitation requires that OpenSSL is compiled using the TLS server name

extensions.

2) An unspecified error can be exploited by a malicious server to crash a client application when the "Server Key exchange message" is omitted from a TLS handshake.

The vulnerabilities are reported in versions 0.9.8f and 0.9.8g.

References:

http://www.openssl.org/news/secadv_20080528.txt

Samba "receive_smb_raw()" Buffer Overflow Vulnerability

"Execution of arbitrary code"

Secunia Research has discovered a vulnerability in Samba, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the "receive_smb_raw()" function in lib/util_sock.c when parsing SMB packets. This can be exploited to cause a heap-based buffer overflow via an overly large SMB packet received in a client context.

Successful exploitation allows execution of arbitrary code by tricking a user into connecting to a malicious server (e.g. by clicking an "smb://" link) or by sending specially crafted packets to an "nmbd" server configured as a local or domain master browser.

The vulnerability is confirmed in versions 3.0.28a and 3.0.29. Prior versions may also be affected.

References:

http://secunia.com/secunia_research/2008-20/

Trillian Multiple Vulnerabilities

"Execution of arbitrary code"

Some vulnerabilities have been reported in Trillian, which can be exploited by malicious people to compromise a user's system.

1) A boundary error within the header parsing code for the MSN protocol can be exploited to cause a stack-based buffer overflow via a specially crafted X-MMS-IM-FORMAT header with an overly long attribute.

Successful exploitation allows execution of arbitrary code.

2) An error within the XML parsing in talk.dll can be exploited to cause a memory corruption via certain malformed attributes within an 'IMG' tag.

Successful exploitation allows execution of arbitrary code.

3) A boundary error when parsing messages (e.g. via the AIM network) with overly long attribute values within the FONT tag can be exploited to cause a stack-based buffer overflow.

Successful exploitation allows execution of arbitrary code but requires that the user is tricked into opening a malicious image file.

References:

<http://www.zerodayinitiative.com/advisories/ZDI-08-031/>
<http://www.zerodayinitiative.com/advisories/ZDI-08-030/>
<http://www.zerodayinitiative.com/advisories/ZDI-08-029/>

Cisco IOS SSH Server Denial of Service

“Denial of Service”

Some vulnerabilities have been reported in Cisco IOS, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerabilities are caused due to unspecified errors within the SSH server implementation in Cisco IOS. These can be exploited to generate a spurious memory access or to reload the device.

Successful exploitation requires that the SSH server is enabled (not enabled by default).

The vulnerabilities are reported in certain 12.4-based IOS releases.

NOTE: IOS releases prior to 12.4(7), 12.4(13d)JA, and 12.4(9)T are reportedly not affected by this vulnerability.

References:

<http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>

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@seccurescout.net