netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 31

August 10, 2007

Table of Contents

Product Focus

Messenger Service Vulnerability Scanner – The Messenger Service 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 Microsoft Windows Messenger Service flaw (MS03-043).

This Week in Review

PCI compliance coming along slowly.Cisco users: Be aware.Tihis years bad good news from Black Hat.England working on laws for online security.

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

- **The Compliance Gamble**

State of compliance

Visa recently released a report on the state of PCI compliance. In general, the statistics seem to suggest forward progress, albeit slower than one might hope for. There is one big cloud over the report though. Some retailers continue to store

sensitive credit card account data that they should not, putting the data in potential jeopardy and creating the conditions for a repeat of the TJX breach.

The good news is that 96% of the large Level 1 and Level 2 merchants claim to be compliant. The bad news is twofold. Firstly, the 96% statistic is based on the number of Level 1 and Level 2 merchants that have written to Visa stating that they are compliant. There is no audit or independent verification of that claim, therefore this statistic may not be accurate. Secondly, even if 96% is correct, that leaves 4% who openly state that they are still retaining magnetic stripe data from credit card transactions.

Visa states that there are 327 Level 1 and 730 Level 2 retailers. If 4% are non-compliant, then 13 Level 1 and 29 Level 2 merchants are still out of PCI compliance when it comes to retaining this data. They are either hoping to be protected by sheer luck, or they are betting that their network security is better than TJX. Either is a game of chance that the retailers are playing with their customers' personal and financial information.

infosecurity

Full Story :
http://www.infosecurity-magazine.com/comment/070810_pci.htm

- **Critical security flaws in IOS warns Cisco**

Cisco is warning customers about multiple vulnerabilities in its Cisco Internework Operating System (IOS) and IOS secure copy server as well as its Unified Communications Manager, which could be exploited remotely by an attacker to conduct a denial of service or execute arbitrary code.

Cisco said multiple vulnerabilities occur in its IOS and Unified Communications Manager when handling malformed Session Initiation Protocol (SIP) packets. SIP is a standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality.

Computerweekly

Full Story :
http://www.computerweekly.com/Articles/2007/08/10/226126/critical-security-flaws-in-ios-warns-cisco.htm

- **Thoughts from Black Hat**

Good info on bad deeds from the Black Hat conference
Talk to anyone who attends Black Hat USA conferences and you'll hear about how boring the talks are, how nobody learned anything new, how the hacks were known last year — not to mention the ridiculous posers. Ask those same attendees if they plan to attend next year, and they say "yeah" as fast as a poker player pushing all in with pocket aces.
I learned that pushing all in with pocket 5s in Las Vegas apparently isn't nearly as smart, but that's another topic.

While many of this year's Black Hat sessions were ultraboring — I walked out of more talks than I stayed in — I learned all sorts of interesting factoids. And although there wasn't, as in the past, any raw meat flying into the audience, some of the speakers were superknowledgeable and entertaining. Here are the ones that seemed to impress the audiences in the sessions I attended:

infoworld

Full Story :
http://www.infoworld.com/article/07/08/10/32OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/08/10/32OPsecadvise_1.html

- **Lords push for wide-ranging security improvements**

Recommendations include the introduction of data security breach notification law in the UK
A new report out today from the House of Lords Science and Technology Committee could lead to a major overhaul of current UK internet security practices, with recommendations ranging from the introduction of a central web-based e-crime reporting system to the introduction of security breach notification laws.

According to the report, the reporting tool would help law enforcement agencies gain an understanding of the computer crime landscape in the UK, and offer a central repository to collate reports and identify patterns.

ITWeek

Full Story :
http://www.itweek.co.uk/itweek/news/2196360/lords-push-wide-ranging

New Vulnerabilities Tested in SecureScout

- **16573 Multiple Cisco IOS IPS Vulnerabilities (cisco-sa-20070213-iosips)**

The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

* Fragmented IP packets may be used to evade signature inspection.
* IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

Fragmented Packet Evasion Vulnerability

Some of the IPS signatures utilize regular expressions. Due to a vulnerability, an attacker can evade those IPS signatures by sending malicious network traffic as IP fragments. This may result in potential malicious traffic bypassing signature inspection and possibly allow the exploitation of protected systems. IPS signatures which do not utilize regular expressions are not affected by this vulnerability. All IP protocols (e.g. TCP, UDP, ICMP) are affected by this vulnerability. There is a mitigation for this vulnerability. This vulnerability is documented in Cisco Bug ID CSCsg15598 (registered customers only) .

ATOMIC.TCP Regular Expression Denial of Service Vulnerability

Certain network traffic can trigger IPS signatures which use the regular expression feature of the ATOMIC.TCP signature engine which may cause the IOS IPS device to crash. This may cause a denial of service resulting in disruption network traffic. Signature 3123.0 (Netbus Pro Traffic) has been demonstrated to trigger this vulnerability. There is a workaround for this vulnerability. This vulnerability is documented in Cisco Bug ID CSCsa53334 (registered customers only) .

The issue has been fixed in Firefox 2.0.0.5.

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

References:

References:
* CISCO: cisco-sa-20070213-iosips
http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml

CVE Reference:

- **16572 Cisco Crafted IP Option Vulnerability (cisco-sa-20070124-crafted-ip-option)**

Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

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

References:

* CISCO: cisco-sa-20070124-crafted-ip-option
http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

CVE Reference:

- **16571 Cisco IPv6 Routing Header Vulnerability (cisco-sa-20070124-IOS-IPv6)**

Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

This vulnerability was initially reported by a customer and further trigger vector was discovered during developing the fix for this vulnerability.

The issue has been fixed in version 7.2.0.

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

References:

* CISCO: cisco-sa-20070124-IOS-IPv6
http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

CVE Reference:

- **16570 Multiple Vulnerabilities in the Cisco IOS FTP Server (cisco-sa-20070509-iosftp)**

The Cisco IOS FTP Server feature contains multiple vulnerabilities that can result in a denial of service (DoS) condition, improper verification of user credentials, and the ability to retrieve or write any file from the device filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the IOS FTP Client feature.

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

References:

* CISCO: cisco-sa-20070509-iosftp
http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml

CVE Reference:

❖ 16569 Multiple Vulnerabilities in Cisco IOS While Processing SSL Packets (cisco-sa-20070522-SSL)

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

* Processing ClientHello messages, documented as Cisco bug ID CSCsb12598 (registered customers only)
* Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304 (registered customers only)
* Processing Finished messages, documented as Cisco bug ID CSCsd92405 (registered customers only)

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

References:

* CISCO: cisco-sa-20070522-SSL
http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

CVE Reference:

❖ 16568 Cisco IOS Vulnerability In Crypto Library (cisco-sa-20070522-crypto)

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

* Cisco IOS
* Cisco IOS XR

* Cisco PIX and ASA Security Appliances
* Cisco Firewall Service Module (FWSM)
* Cisco Unified CallManager

This vulnerability is assigned CVE ID CVE-2006-3894. It is externally coordinated and is tracked by the following external coordinators:

* JPCERT/CC - tracked as JVNVU#754281
* CPNI - tracked as NISCC-362917
* CERT/CC - tracked as VU#754281

The issue has been fixed in version 7.2.0.

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

References:

* CISCO: cisco-sa-20070522-crypto
http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml
* CONFIRM:
http://jvn.jp/cert/JVNVU%23754281/index.html
* CONFIRM:
https://secure-support.novell.com/KanisaPlatform/Publishing/97/3590033_f.SAL_Public.html
* CISCO: 20070522 Vulnerability in Crypto Library
http://www.cisco.com/en/US/products/products_security_advisory09186a0080847c5d.shtml
* CERT-VN: VU#754281
http://www.kb.cert.org/vuls/id/754281
* BID: 24104
http://www.securityfocus.com/bid/24104
* FRSIRT: ADV-2007-1908
http://www.frsirt.com/english/advisories/2007/1908
* FRSIRT: ADV-2007-1909
http://www.frsirt.com/english/advisories/2007/1909
* FRSIRT: ADV-2007-1945
http://www.frsirt.com/english/advisories/2007/1945
* SECTRACK: 1018095
http://www.securitytracker.com/id?1018095
* SECUNIA: 25364
http://secunia.com/advisories/25364
* SECUNIA: 25399
http://secunia.com/advisories/25399
* SECUNIA: 25343
http://secunia.com/advisories/25343
* XF: cisco-crypto-asn1-dos(34430)
http://xforce.iss.net/xforce/xfdb/34430

CVE Reference: CVE-2006-3894

❖ **16567 Cisco IOS Secure Copy Authorization Bypass Vulnerability (cisco-sa-20070808-scp)**

The server side of the Secure Copy (SCP) implementation in Cisco Internetwork Operating System (IOS) contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS Secure Copy Server service are not affected by this vulnerability.

This vulnerability does not apply to the IOS Secure Copy Client feature.

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

References:

* CISCO: cisco-sa-20070808-scp
http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

CVE Reference:

❖ 16566 Cisco IOS Next Hop Resolution Protocol Vulnerability (cisco-sa-20070808-nhrp)

The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

NHRP is not enabled by default for Cisco IOS.

This vulnerability is addressed by Cisco bug IDs CSCin95836 (registered customers only) for non-12.2 mainline releases and CSCsi23231 (registered customers only) for 12.2 mainline releases.

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

References:

* CISCO: cisco-sa-20070808-nhrp
http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

CVE Reference:

❖ 16412 Cisco IOS Information Leakage Using IPv6 Routing Header (cisco-sa-20070808-IOS-IPv6-leak)

Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected IOS and IOS XR devices, and may also result in a crash of the affected IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

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

References:

* CISCO: cisco-sa-20070808-IOS-IPv6-leak
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml

CVE Reference:

❖ 16263 Voice Vulnerabilities in Cisco IOS and Cisco Unified Communications Manager (cisco-sa-20070808-IOS-voice)

SIP-related vulnerabilities

SIP is a protocol that is used to establish, modify, and terminate multimedia sessions. Most commonly, SIP is used for Internet telephony. SIP call signaling can use UDP (User Datagram Protocol) or TCP (Transport Control Protocol) as an underlying transport protocol. In all cases vulnerabilities can be triggered by processing a malformed SIP packet.

A malformed SIP packet may cause a vulnerable device to crash and may allow arbitrary code to be executed. These vulnerabilities are documented as the following Cisco Bug IDs:

* CSCsi80749 Crash while processing malformed SIP packet (registered customers only)
* CSCsi80102 CUCM - Crash while processing malformed SIP packet (registered customers only)

A malformed SIP packet may cause a memory leak and device crash. These vulnerabilities are documented as the following Cisco Bug IDs:

* CSCsf11855 Crash while processing malformed SIP packet (registered customers only)
* CSCeb21064 Crash while processing malformed SIP packet (registered customers only)
* CSCse40276 Router crashed by malformed SIP message (registered customers only)
* CSCse68355 Router crashed by malformed SIP packet (registered customers only)
* CSCsf30058 Memory leak when processing malformed SIP message (registered customers only)
* CSCsb24007 Memory corruption and unexpected reload on receiving a SIP packet (registered customers only)
* CSCsc60249 Crash while processing malformed SIP packet (registered customers

only)

MGCP-related vulnerabilities

MGCP is a protocol for controlling media gateways from external call control elements such as Media Gateway Controllers or Call Agents. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. In a Cisco environment, a media gateway is used between the Cisco Communications Manager and the Cisco router and servers as a voice gateway.

A specially crafted MGCP packet can cause a vulnerable device to crash or become unresponsive. The unresponsive device will not be able to establish new telephone calls, and a reboot is required to restore normal operation. These vulnerabilities are documented as the following Cisco Bug IDs:

* CSCsf08998 MGCP stop responding after receiving malformed packet (registered customers only)
* CSCsd81407 Router crash on receiving abnormal MGCP messages (registered customers only)

H.323-signaling related vulnerabilities

H.323 is an ITU (International Telecommunications Union) set of recommendations for multimedia communication and signaling in networks that use Internet Protocol.

A malformed H.323 packet can crash a vulnerable device. These vulnerabilities are documented as the following Cisco Bug IDs:

* CSCsi60004 H323 Proxy Unregistration from Gatekeeper (registered customers only)
* CSCsg70474 IOS FW with h323 inspect crashes when malformed H.323 packets received (registered customers only)

Real-time Transport Protocol-related vulnerabilities

RTP is a protocol that is designed to provide delivery services for data with real-time characteristics, such as interactive audio and video.

A malformed RTP packet can cause a vulnerable device to crash. These vulnerabilities are documented as the following Cisco Bug IDs:

* CSCse68138 Issue in handling specific packets in VOIP RTP Lib (registered customers only)
* CSCse05642 I/O memory corruption crash on a router (registered customers only)

Facsimile reception vulnerability

Reception of a large packet can cause a vulnerable device to crash. This vulnerability is documented as the following Cisco Bug ID:

* CSCej20505 Router hangs with overly large packet (registered customers only)

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

References:

* CISCO: cisco-sa-20070808-IOS-voice
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CVE Reference:

New Vulnerabilities found this Week

Symantec Products NavComUI ActiveX Control Code Execution

"Execution of arbitrary code"

Secunia Research has discovered two vulnerabilities in various Symantec products, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to errors in the AxSysListView32 and AxSysListView32OAA ActiveX controls (NavComUI.dll) when handling the "AnomalyList" and "Anomaly" properties respectively as they take a VARIANT* as argument.

Successful exploitation allows execution of arbitrary code.

The vulnerabilities have been confirmed in Norton Internet Security 2006 including Norton AntiVirus 12.7.0.2. According to the vendor, the following versions are affected:
* Norton AntiVirus 2006
* Norton Internet Security 2006
* Norton Internet Security, Anti Spyware Edition 2005
* Norton System Works 2006

References:
http://www.symantec.com/avcenter/security/Content/2007.08.09.html

gFTP Multiple Vulnerabilities

"Execution of arbitrary code"

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

The vulnerabilities are caused due to the use of vulnerable fsplib code, which may allow the execution of arbitrary code.

References:
http://secunia.com/advisories/26184/

Cisco IOS Voice Service Multiple Protocol Handling Vulnerabilities

"Denial of service; Crash; Code execution"

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

* Session Initiation Protocol (SIP)
* Media Gateway Control Protocol (MGCP)
* Signaling protocols H.323, H.254
* Real-time Transport Protocol (RTP)
* Facsimile reception

References:
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml
http://descriptions.securescout.com/tc/16263

Cisco IOS Information Leakage Using IPv6 Routing Header (cisco-sa-20070808-IOS-IPv6-leak)

"Denial of service; Crash; Code execution"

Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected IOS and IOS XR devices, and may also result in a crash of the affected IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml
http://descriptions.securescout.com/tc/16412

Cisco IOS Next Hop Resolution Protocol Vulnerability (cisco-sa-20070808-nhrp)

"Denial of service; Crash; Code execution"

The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

NHRP is not enabled by default for Cisco IOS.

This vulnerability is addressed by Cisco bug IDs CSCin95836 (registered customers only) for non-12.2 mainline releases and CSCsi23231 (registered customers only) for 12.2 mainline releases.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml
http://descriptions.securescout.com/tc/16566

Cisco IOS Secure Copy Authorization Bypass Vulnerability (cisco-sa-20070808-scp)

“Denial of service; Crash; Code execution”

The server side of the Secure Copy (SCP) implementation in Cisco Internetwork Operating System (IOS) contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS Secure Copy Server service are not affected by this vulnerability.

This vulnerability does not apply to the IOS Secure Copy Client feature.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml
http://descriptions.securescout.com/tc/16567

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