netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 33

August 24, 2007

Table of Contents

Product Focus

netVigilance has ported Honeyd 1.5c to Windows, and released it for free under the name WinHoneyd.
The complete source and the compiled executable are available for free on our web-site.
The update from winhoneyd 1.5b to 1.5c is mainly a bugfix /code optimization release.
To download WinHoneyd.exe or the WinHoneyd source please visit
http://www.netvigilance.com/winhoneyd

Infoworld writes about Honeypots: Jesper Jurcenoks, co-founder of netVigilance, has released an updated version of Honeyd for Windows. You can get it at the netVigilance Web site. Jesper and his company took the time to do a complete rewrite and free update of Honeyd for Windows. He even corrected one bug that remains in the Linux/Unix version to make sure it didn't get replicated to the Windows version, and netVigilance offers a $99 GUI configurator, which can save you hours of configuring and troubleshooting. Thanks to Jesper and netVigilance (and Michael Davis for his earlier contributions) for allowing us Windows security types to play with Niels' excellent honeypot software.

For more, check out http://www.infoworld.com/article/07/08/24/34OPsecadvise_1.html

Nimda Worm Scanner – The Nimda Worm 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 MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

This Week in Review

A guide to patching. Risky behavioural trends among mobile computing users. The

hyperconnected employee. New book on fuzzing techniques.

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

❖ How to patch five must-close vulnerabilities, now

Neutralizing today's worst Web attacks
Symantec Corp. recently posted details about a new version of MPack, a for-sale Web attack kit that loads up a site with exploits against Windows, QuickTime and WinZip. The $400 kit was used in the June Italian Job online assault that hijacked tens of thousands of Web sites, most of them in Italy. Crooks can buy MPack and a host of other nefarious programs on a thriving online black market.

In its post, Symantec listed only which holes the new MPack version targets; I followed up with the company to get specifics and links to fixes. All of the vulnerabilities allow an attacker to take over your PC if you view a tainted Web page. And according to Roger Thompson of Exploit Prevent Labs, another popular kit called Icepack attacks the same flaws.

Since thousands of poisoned Web sites actively attack these program vulnerabilities, they are must-close holes -- and making sure they're fixed will go a good ways toward keeping you safe online.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9032338&taxonomyId=17&intsrc=kc_feat

❖ Mobile workers take too many security risks

Survey uncovers some risky behavioural trends among laptop and other mobile computing users.
A global study into mobile workers' attitudes to IT security suggests there is still much work to be done in raising awareness of security threats and best practices while working on the move.

The survey, carried out by market researcher InsightExpress, found almost three quarters (73 per cent) of mobile users claimed that they were not always mindful of security issues. Although many said they are aware "sometimes" of the risks and threats, 28 per cent admitted that they "hardly ever" consider security risks and proper behaviour.

More worryingly, some of the 700 mobile users surveyed for the study commissioned by Cisco and the National Cyber Security Alliance (NCSA) even admitted that they "never"

consider safe best practices and didn't know they needed to be aware of security risks.

ITPro

Full Story :
http://www.itpro.co.uk/news/123227/mobile-workers-take-too-many-security-risks.html

❖ Hyperconnection comment

Businesses should welcome the use of social networks but ensure policies are in place to protect company equipment, according to virus IT staff at DriveSentry.
The rapid growth in popularity of sites such as Facebook and MySpace has meant that many organisations are attempting to add them to their 'banned sites' list. But even that will do little to protect against malicious use in the era of 'hyperconnection', according to John Safa, Chief Technology Officer at DriveSentry.

"The use of social networks in combination with flexible working policies and ubiquitous broadband connectivity will see many more viruses slipping through the net of traditional anti-virus products," said John. "Users are now hyperconnected, and as a result the number of opportunities for malware to be unwittingly downloaded has grown exponentially."

Proffessionel security magazine

Full Story :
http://www.professionalsecurity.co.uk/newsdetails.aspx?NewsArticleID=7584&imgID=1

❖ Information security book excerpts and reviews

Fuzzing: Brute Force Vulnerability Discovery
Written by Michael Sutton, Adam Greene and Pedram Amini
Published by Addison-Wesley
Fuzzing has evolved into one of today's most effective approaches to test software security, and this book introduces state-of-the-art fuzzing techniques that can find vulnerabilities in network protocols, file formats and Web applications. Throughout each chapter, the three authors also present several insightful case histories that show the bug-finding technique at work.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2007/06/12/216855/information-security-book-excerpts-and-reviews.htm

New Vulnerabilities Tested in SecureScout

❖ 16597 Windows VPN Client Local Privilege Escalation Vulnerability (cisco-sa-20060524-vpnclient) (Remote File Checking)

The Cisco VPN Client for Windows is affected by a local privilege escalation vulnerability that allows non-privileged users to gain administrative privileges.

A user needs to authenticate and start an interactive Windows session to be able to exploit this vulnerability.

The issues are discussed in bug CSCsd79265.

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

References:

* CISCO: 20060524 Windows VPN Client Local Privilege Escalation Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a008069a323.shtml
* BID: 18094
http://www.securityfocus.com/bid/18094
* FRSIRT: ADV-2006-1964
http://www.frsirt.com/english/advisories/2006/1964
* OSVDB: 25888
http://www.osvdb.org/25888
* SECTRACK: 1016156
http://securitytracker.com/id?1016156
* SECUNIA: 20261
http://secunia.com/advisories/20261
* XF: cisco-winvpn-privilege-escalation(26632)
http://xforce.iss.net/xforce/xfdb/26632
* CISCO: cisco-sa-20060524-vpnclient
http://www.cisco.com/warp/public/707/cisco-sa-20060524-vpnclient.shtml

CVE Reference: CVE-2006-2679

❖ 16596 BIND dereferencing freed fetch context Vulnerability

It is possible for the named to dereference (read) a freed fetch context. This can cause named to exit unintentionally.

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

References:

* BUGTRAQ: 20070125 BIND remote exploit (low severity) [Fwd: Internet Systems Consortium Security Advisory.]
http://www.securityfocus.com/archive/1/archive/1/458066/100/0/threaded
* FULLDISC: 20070125 BIND remote exploit (low severity) [Fwd: Internet Systems Consortium Security Advisory.]
http://lists.grok.org.uk/pipermail/full-disclosure/2007-January/052018.html
* MLIST: [bind-announce] 20070125 Internet Systems Consortium Security Advisory.
http://marc.theaimsgroup.com/?l=bind-announce&m=116968519321296&w=2

CVE Reference: CVE-2007-0493

❖ 16595 BIND DNSSEC Validation Vulnerability

When validating responses to type * (ANY) queries that return multiple RRsets in the answer section it is possible to trigger assertions checks. To be vulnerable you need to have enabled dnssec validation in named.conf by specifying trusted-keys.

Note:
It is recommended that anyone using DNSSEC upgrade to BIND 9.3 as the DNSSEC implementation in BIND 9.2 has been obsoleted.

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

References:

* MLIST: [bind-announce] 20070125 Internet Systems Consortium Security Advisory.
http://marc.theaimsgroup.com/?l=bind-announce&m=116968519300764&w=2
* CONFIRM:
http://www.isc.org/index.pl?/sw/bind/bind-security.php
* CONFIRM:
http://www.isc.org/index.pl?/sw/bind/view/?release=9.2.8
* CONFIRM:
http://www.isc.org/index.pl?/sw/bind/view/?release=9.3.4
* CONFIRM:
https://issues.rpath.com/browse/RPL-989
* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2007-125.htm
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=305530

CVE Reference: CVE-2007-0494

❖ 16594 Local Privilege Escalation Vulnerabilities in Cisco VPN Client (cisco-sa-20070815-vpnclient) (Remote File Checking)

Two vulnerabilities exist in the Cisco VPN Client for Microsoft Windows that may allow unprivileged users to elevate their privileges to those of the LocalSystem account.

A workaround exists for one of the two vulnerabilities disclosed in this advisory.

The issues are discussed in the following bugs:
1. Local Privilege Escalation Through Microsoft Windows Dial-Up Networking Interface CSCse89550.

2. Local Privilege Escalation Through Default cvpnd.exe File Permissions CSCsj00785.

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

References:

* CISCO: cisco-sa-20070815-vpnclient
http://www.cisco.com/warp/public/707/cisco-sa-20070815-vpnclient.shtml
* BID: 25332
http://www.securityfocus.com/bid/25332
* FRSIRT: ADV-2007-2903
http://www.frsirt.com/english/advisories/2007/2903
* SECTRACK: 1018573
http://securitytracker.com/id?1018573
* SECUNIA: 26459
http://secunia.com/advisories/26459
* XF: cisco-vpn-dialup-privilege-escalation(36029)
http://xforce.iss.net/xforce/xfdb/36029
* BUGTRAQ: 20070816 Local privilege escalation vulnerability in Cisco VPN client
http://www.securityfocus.com/archive/1/archive/1/476812/100/0/threaded
* XF: cisco-vpn-cvpnd-privilege-escalation(36032)
http://xforce.iss.net/xforce/xfdb/36032

CVE Reference: CVE-2007-4414

❖ 16593 DLSw Vulnerability (cisco-sa-20070110-dlsw)

A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

This issue is documented as Cisco bug ID CSCsf28840.

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

References:

* CISCO: cisco-sa-20070110-dlsw
http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml
* BID: 21990
http://www.securityfocus.com/bid/21990
* FRSIRT: ADV-2007-0139
http://www.frsirt.com/english/advisories/2007/0139
* SECTRACK: 1017498
http://securitytracker.com/id?1017498
* SECUNIA: 23697
http://secunia.com/advisories/23697

CVE Reference: CVE-2007-0199

❖ 16592 Crafted TCP Packet Can Cause Denial of Service (cisco-sa-20070124-crafted-tcp)

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a

denial of service condition.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

This issue is documented as Cisco bug ID CSCek37177.

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

References:

* CISCO: cisco-sa-20070124-crafted-tcp
http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml
* CISCO: 20070124 Crafted TCP Packet Can Cause Denial of Service
http://www.cisco.com/en/US/products/products_security_advisory09186a00807cb0e4.shtml
* CERT-VN: VU#217912
http://www.kb.cert.org/vuls/id/217912
* BID: 22208
http://www.securityfocus.com/bid/22208
* FRSIRT: ADV-2007-0329
http://www.frsirt.com/english/advisories/2007/0329
* SECTRACK: 1017551
http://securitytracker.com/id?1017551
* SECUNIA: 23867
http://secunia.com/advisories/23867
* XF: cisco-tcp-ipv4-dos(31716)
http://xforce.iss.net/xforce/xfdb/31716

CVE Reference: CVE-2007-0479

❖ 16591 SIP Packets Reload IOS Devices with support for SIP (cisco-sa-20070131-sip)

Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

The following bugs discuss the issue:
CSCsb25337 - unnecessary tcp ports opened in default router config
CSCsh58082 - SIP: A router may reload due to SIP traffic

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

References:

* CONFIRM:
http://www.cisco.com/warp/public/707/cisco-air-20070131-sip.shtml
* CISCO: cisco-sa-20070131-sip
http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml
* CERT-VN: VU#438176
http://www.kb.cert.org/vuls/id/438176
* BID: 22330
http://www.securityfocus.com/bid/22330
* FRSIRT: ADV-2007-0428
http://www.frsirt.com/english/advisories/2007/0428
* SECTRACK: 1017575
http://securitytracker.com/id?1017575
* SECUNIA: 23978
http://secunia.com/advisories/23978
* XF: cisco-sip-packet-dos(31990)
http://xforce.iss.net/xforce/xfdb/31990

CVE Reference: CVE-2007-0648

❖ 16590 Cisco Catalyst 6000, 6500 and Cisco 7600 Series MPLS Packet Vulnerability (cisco-sa-20070228-mpls)

Cisco Catalyst 6500 series systems that are running certain versions of Cisco Internetwork Operating System (IOS) are vulnerable to an attack from a Multi Protocol Label Switching (MPLS) packet. Only the systems that are running in Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the Multilayer Switch Feature Card (MSFC)) or running with Cisco IOS Software Modularity are affected.

MPLS packets can only be sent from the local network segment.

Triggering this vulnerability may result in a Denial of Service.

This issue is documented in bug IDs CSCsd37415 and CSCef90002.

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

References:

* CISCO: cisco-sa-20070228-mpls
http://www.cisco.com/warp/public/707/cisco-sa-20070228-mpls.shtml
* FRSIRT: ADV-2007-0782
http://www.frsirt.com/english/advisories/2007/0782
* SECTRACK: 1017709
http://www.securitytracker.com/id?1017709
* SECUNIA: 24348
http://secunia.com/advisories/24348
* XF: cisco-catalyst-mpls-dos(32748)
http://xforce.iss.net/xforce/xfdb/32748

CVE Reference: CVE-2007-1258

❖ 16589 Cisco Catalyst 6000, 6500 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability (cisco-sa-20070228-nam) (CatOS)

NAMs are deployed in Catalyst 6000, 6500 series and Cisco 7600 series to monitor and analyze network traffic by using Remote Monitoring (RMON), RMON2, and other MIBs.

NAMs communicate with the Catalyst system by using the Simple Network Management Protocol (SNMP). By spoofing the SNMP communication between the Catalyst system and the NAM an attacker may obtain complete control of the Catalyst system.

Devices running both Cisco IOS and Cisco CatOS are affected by this vulnerability. This vulnerability is introduced in CatOS at 7.6(15) and 8.5(1). Older CatOS images are not vulnerable.

This issue is documented in bug IDs CSCsd75273, CSCse52951, CSCse39848.

This particular Test Case only check devices running CatOS.

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

References:

* CISCO: cisco-sa-20070228-nam
http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml
* CERT-VN: VU#472412
http://www.kb.cert.org/vuls/id/472412
* BID: 22751
http://www.securityfocus.com/bid/22751
* FRSIRT: ADV-2007-0783
http://www.frsirt.com/english/advisories/2007/0783
* SECTRACK: 1017710
http://www.securitytracker.com/id?1017710
* SECUNIA: 24344
http://secunia.com/advisories/24344
* XF: cisco-catalyst-nam-unauthorized-access(32750)
http://xforce.iss.net/xforce/xfdb/32750

CVE Reference: CVE-2007-1257

❖ 16588 Cisco Catalyst 6000, 6500 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability (cisco-sa-20070228-nam) (IOS)

NAMs are deployed in Catalyst 6000, 6500 series and Cisco 7600 series to monitor and analyze network traffic by using Remote Monitoring (RMON), RMON2, and other MIBs.

NAMs communicate with the Catalyst system by using the Simple Network Management Protocol (SNMP). By spoofing the SNMP communication between the Catalyst system and the NAM an attacker may obtain complete control of the Catalyst system.

Devices running both Cisco IOS and Cisco CatOS are affected by this vulnerability. This vulnerability is introduced in CatOS at 7.6(15) and 8.5(1). Older CatOS images are not vulnerable.

This issue is documented in bug IDs CSCsd75273, CSCse52951, CSCse39848.

This particular Test Case only check devices running IOS.

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

References:

References:
* CISCO: cisco-sa-20070228-nam
http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml
* CERT-VN: VU#472412
http://www.kb.cert.org/vuls/id/472412
* BID: 22751
http://www.securityfocus.com/bid/22751
* FRSIRT: ADV-2007-0783
http://www.frsirt.com/english/advisories/2007/0783
* SECTRACK: 1017710
http://www.securitytracker.com/id?1017710
* SECUNIA: 24344
http://secunia.com/advisories/24344
* XF: cisco-catalyst-nam-unauthorized-access(32750)
http://xforce.iss.net/xforce/xfdb/32750

CVE Reference: CVE-2007-1257

New Vulnerabilities found this Week

Cisco IP Phone 7940/7960 SIP Message Sequence Denial of Service

"Denial of Service"

The Madynes research team at INRIA Lorraine has reported some vulnerabilities in Cisco IP Phone 7940 and 7960, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerabilities are caused due to errors within the handling of certain SIP message sequences. These can be exploited to reboot the device by sending a series of specially crafted SIP messages.

The vulnerabilities are reported in firmware version POS3-08-6-00.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-August/065401.html
http://lists.grok.org.uk/pipermail/full-disclosure/2007-August/065402.html

http://www.cisco.com/en/US/products/products_security_response09186a00808a6693.html

ClamAV Multiple Denial of Service Vulnerabilities

"Denial of Service"

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

1) A NULL-pointer dereference error exists within the "cli_scanrtf()" function in libclamav/rtf.c. This can potentially be exploited to crash ClamAV via a specially crafted RTF file.

2) A NULL-pointer dereference error exists within the "cli_html_normalise()" function in libclamav/htmlnorm.c. This can potentially be exploited to crash ClamAV via a specially crafted HTML file containing a "data" URL scheme.

The vulnerabilities are reported in versions prior to 0.91.2.

References:
http://sourceforge.net/project/shownotes.php?release_id=533658&group_id=86638

Trend Micro ServerProtect Multiple Buffer Overflow Vulnerabilities

"Execution of arbitrary code"

Some vulnerabilities have been reported in Trend Micro ServerProtect, which can be exploited by malicious people to compromise a vulnerable system.

1) An integer overflow error within the RPCFN_SYNC_TASK function in StRpcSrv.dll can be exploited to cause a heap-based buffer overflow via a specially crafted RPC request to SpntSvc.exe on default port 5168/TCP.

2) Boundary errors within the RPCFN_ENG_NewManualScan, RPCFN_ENG_TimedNewManualScan, and RPCFN_SetComputerName functions in StRpcSrv.dll can be exploited to cause stack-based buffer overflows via specially crafted RPC requests to SpntSvc.exe on default port 5168/TCP.

3) Boundary errors within the RPCFN_CMON_SetSvcImpersonateUser and RPCFN_OldCMON_SetSvcImpersonateUser functions in Stcommon.dll can be exploited to cause stack-based buffer overflows via specially crafted RPC requests to SpntSvc.exe on default port 5168/TCP.

4) Boundary errors within the RPCFN_ENG_TakeActionOnAFile and RPCFN_ENG_AddTaskExportLogItem functions in Eng50.dll can be exploited to cause heap- and stack-based buffer overflows via specially crafted RPC requests to SpntSvc.exe on default port 5168/TCP.

5) A boundary error within the NTF_SetPagerNotifyConfig function in Notification.dll can be exploited to cause a stack-based buffer overflow via a specially crafted RPC request to SpntSvc.exe on default port 5168/TCP.

6) A boundary error within the RPCFN_CopyAUSrc function in the Trend ServerProtect Agent service can be exploited to cause a stack-based buffer overflow via a specially

crafted RPC request sent to default port 3628/TCP.

7) Boundary errors within the RPCFN_EVENTBACK_DoHotFix and CMD_CHANGE_AGENT_REGISTER_INFO in earthagent.exe can be exploited to cause buffer overflows.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

The vulnerabilities are reported in ServerProtect for Windows version 5.58 Build 1176. Other versions may also be affected.

References:
http://www.trendmicro.com/ftp/documentation/readme/spnt_558_win_en_securitypatch4_readme.txt
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=588
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=587

Yahoo! Messenger Webcam JPEG 2000 Processing Vulnerabilities

"Denial of Service"

Two vulnerabilities have been reported in Yahoo! Messenger, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a user's system.

The vulnerabilities are caused due to input validation errors in ywcvwr.dll and kdu_v32m.dll when processing JPEG 2000 streams sent via the webcam stream. These can be exploited to cause a DoS condition or a heap-based buffer overflow when a user e.g. is tricked into viewing a malicious webcam stream.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities affects all versions downloaded before August 21, 2007.

References:
http://secunia.com/software_inspector/
http://messenger.yahoo.com/security_update.php?id=082107
https://www.xfocus.net/bbs/index.php?act=ST&f=2&t=64639&page=1#entry321749
http://www.kb.cert.org/vuls/id/515968

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.

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