netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 34

August 31 , 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

RPC DCOM Vulnerabilities Scanner – The RPC DCOM Vulnerabilities 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 RPC DCOM flaws (MS03-026 and MS03-039).

This Week in Review

xxx.

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

- **10 reasons to be paranoid**

Every bit of your virtual existence is being monitored -- get scared accordingly
The truth is out there ... and so is your data. And just because there are no virtual black helicopters following you doesn't mean somebody somewhere doesn't have a bead on who you are and what you are doing.
From buttinski bosses to spies and spooks, there are plenty of reasons to be, well, a little paranoid about the vulnerability of your data and the potential loss of your privacy. To help you gauge the appropriate level of hysteria, we've rated each threat on our Paranoia Meter, using a scale of 1 (Don't worry, be happy) to 5 (Be afraid, be very afraid). Though we've taken a lighthearted approach, concerns about data privacy are not all fun and games.

"You can look at 'paranoia' as just a good way of having a long horizon," says Jim Harper, director of information policy studies at the Cato Institute. "Incentives exist for data practices to be abused very badly in the future. Being paranoid about them today is being rational about protecting yourself tomorrow."

Infoworld

Full Story :
http://www.infoworld.com/article/07/08/27/35FEparanoia-index_1.html

- **Official databases fail to protect personal data**

Organisations face challenge in protecting confidential records
Official organisations that maintain databases containing personal information need to devise better ways to protect individuals' privacy while preserving the value of the information to researchers, academics argue.

A report by Carnegie Mellon University statistics professor George Duncan in the journal Science claimed that traditional methods of 'de-identifying' records, such as stripping away Social Security numbers or birthdates, are inadequate to safeguard privacy.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2197764/personal-official-databases

- **OOXML approval system open to abuse**

Lack of Integrity
It is hard to consider the current high drama of Office Open XML and the International Organization for Standardization as anything other than a global soap opera. From Ghana, reports of "anti-Microsoft fundamentalism" being used as an argument against technical objections. From India, complaints that "we didn't oppose ODF, so why are you opposing OOXML?". And from Sweden, more than 20 new companies, overwhelmingly Microsoft partners, joining the committee voting on ISO certification within days of the final vote.

Whether or not OOXML is a good candidate for an open standard is beside the point: there is prima facie evidence of voting in bad faith, without proper consideration of all the aspects of the proposal. This is not something that can be fixed later; there are severe implications for the industry in adopting a standard that has not been fully analysed. Those who vote without understanding what they vote for, or because they have primarily political or commercial reasons, are guilty of subverting the process.

zdnet

Full Story :
http://news.zdnet.co.uk/leader/0,1000002982,39288965,00.htm

- **Malicious Web: Not just porn sites**

Seven surprises from Honeypot project show any content can sting, and patching is your best defense
The New Zealand Honeynet Project, which produced Capture-HPC (mentioned here last week), also produced an excellent white paper about using Capture-HPC to identify malicious Web servers. On the group's Web site, you'll find that paper, the captured data, and the tools for anyone to inspect and replicate.
The New Zealand Honeynet Project inspected more than 300,000 URLs (nearly 149,000 hosts) for three weeks and found 306 malicious URLs served from 194 malicious servers. Here are the most interesting points, to me:

1. The highest percentage of malicious Web servers were tied directly to adult content. No surprise here. But all types of content (e.g. news or sponsored links) were nearly as bad. It's not like you can just avoid adult sites and be safe.

infoworld

Full Story :
http://www.infoworld.com/article/07/08/31/35OPsecadvise-honeypots-honeyclients-hpc_1.html?source=rss&url=http://www.infoworld.com/article/07/08/31/35OPsecadvise-honeypots-honeyclients-hpc_1.html

New Vulnerabilities Tested in SecureScout

- **16603 MSN Messenger Video Conversation Buffer Overflow Vulnerability (Remote File Checking)**

Yahoo! Messenger is a free instant messaging software.

wushi has reported a vulnerability in MSN Messenger, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the handling of video conversations and can be exploited to cause a heap-based buffer overflow via specially crafted data sent to a user.

Successful exploitation may allow execution of arbitrary code, but requires that the victim accepts the incoming Web Cam invitation.

The vulnerability is reported in version 7.x. Other versions may also be affected.

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

References:

* MISC:
http://www.team509.com/modules.php?name=News&file=article&sid=50
* SECUNIA: 26570
http://secunia.com/advisories/26570/
* SECTRACK: 1018622
http://www.securitytracker.com/alerts/2007/Aug/1018622.html
* CIAC:
http://www.ciac.org/ciac/bulletins/r-332.shtml

CVE Reference: CVE-2007-2931

❖ 16602 Yahoo! Messenger Filename Buffer Overflow Vulnerability (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

Tri Huynh has reported a vulnerability in Yahoo! Messenger, allowing malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when handling the filename parameter. An overly long, maliciously crafted filename causes a buffer overflow, which potentially allows execution of arbitrary code with the privileges of the current user.

The vulnerability has been reported in version 5.6.0.1351 and prior.

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

References:

* BUGTRAQ: 20040108 Yahoo Instant Messenger Long Filename Downloading Buffer Overflow
http://marc.theaimsgroup.com/?l=bugtraq&m=107357996802255&w=2
* FULLDISC: 20040108 Yahoo Instant Messenger Long Filename Downloading Buffer Overflow
http://lists.grok.org.uk/pipermail/full-disclosure/2004-January/015334.html

* BID: 9383
http://www.securityfocus.com/bid/9383

CVE Reference: CVE-2004-0043

❖ 16601 Yahoo! Messenger Conference Invite Denial of Service (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

Gianni Amato has discovered a weakness in Yahoo! Messenger, which can be exploited by malicious people to cause a DoS (Denial of Service).

The weakness is caused due to a NULL pointer dereference error when processing received conference invites. This can be exploited to crash arbitrary users' Yahoo! Messenger clients by sending a Conference Invite packet containing a specially crafted "room name" string.

The vulnerability is confirmed in version 8.0.0.716. Other versions may also be affected.

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:

* BUGTRAQ: 20061025 Re: Yahoo! Messenger Service 18 Remote Buffer Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/449667/100/0/threaded
* FULLDISC: 20061024 Yahoo! Messenger Service 18 Remote Buffer Overflow Vulnerability
http://archives.neohapsis.com/archives/fulldisclosure/2006-10/0518.html
* FULLDISC: 20061026 Re: Yahoo! Messenger Service 18 Remote Buffer Overflow Vulnerability
http://archives.neohapsis.com/archives/fulldisclosure/2006-10/0566.html
* BID: 20625
http://www.securityfocus.com/bid/20625
* FRSIRT: ADV-2006-4193
http://www.frsirt.com/english/advisories/2006/4193
* SECUNIA: 22510
http://secunia.com/advisories/22510

CVE Reference: CVE-2006-5563

❖ 16600 Yahoo! Messenger YMailAttach ActiveX Control Buffer Overflow (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

A vulnerability has been reported in Yahoo! Messenger, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the YMailAttach ActiveX control when handling the TextETACalculating property. This can be exploited to cause a heap-based buffer overflow by setting an overly long string to the said property.

Successful exploitation allows execution of arbitrary code and requires that the user is e.g. tricked into visiting a malicious web site.

The vulnerability is reported in version 8.0 and 7.5. Other versions may also be affected.

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

References:

* CONFIRM:
http://messenger.yahoo.com/security_update.php?id=120806
* CERT-VN: VU#901852
http://www.kb.cert.org/vuls/id/901852
* BID: 21607
http://www.securityfocus.com/bid/21607
* FRSIRT: ADV-2006-5016
http://www.frsirt.com/english/advisories/2006/5016
* SECTRACK: 1017387
http://securitytracker.com/id?1017387
* SECUNIA: 23401
http://secunia.com/advisories/23401

CVE Reference: CVE-2006-6603

❖ 16599 Yahoo! Messenger Contact Details Script Execution Vulnerability (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

Hai Nam Luke has discovered a vulnerability in Yahoo Messenger, which potentially can be exploited by malicious users to compromise a user's system.

Input passed to the "First Name", "Last Name", and "Nickname" fields in the "Contact Details" option is not properly sanitized when displaying status notification messages to the user in a chat box. This can e.g. be exploited to execute a limited amount of arbitrary script code in the Local Zone (My Computer) context by inputting specially crafted image tags in the aforementioned fields, tricking a target user into adding the attacker to the messenger list, sending a message to the target user, and then changing the status e.g. from "Available" to "Invisible To Everyone".

Successful exploitation requires that the attacker is in the messenger list of the target.

NOTE: When a user adds another user to the messenger list, the contact details get truncated, which limits the amount of script code that can be inserted.

The vulnerability is confirmed in version 8.1.0.209. Other versions may also be affected.

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

References:

* BUGTRAQ: 20070126 Cross-site Scripting with Local Privilege Vulnerability in Yahoo Messenger
http://www.securityfocus.com/archive/1/archive/1/458225/100/0/threaded
* BUGTRAQ: 20070127 RE: Cross-site Scripting with Local Privilege Vulnerability in Yahoo Messenger
http://www.securityfocus.com/archive/1/archive/1/458305/100/0/threaded
* BUGTRAQ: 20070127 Re: Cross-site Scripting with Local Privilege Vulnerability in Yahoo Messenger
http://www.securityfocus.com/archive/1/archive/1/458494/100/0/threaded
* BID: 22269
http://www.securityfocus.com/bid/22269
* SECUNIA: 23928
http://secunia.com/advisories/23928

CVE Reference: CVE-2007-0768

❖ 16598 Yahoo! Messenger AudioConf ActiveX Control Buffer Overflow (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

A vulnerability has been reported in Yahoo! Messenger, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the AudioConf ActiveX control (yacscom.dll) component of Yahoo! Messenger. This can be exploited to cause a stack-based buffer overflow by setting the "socksHostname" and "hostName" properties to an overly large string and then calling the "createAndJoinConference()" method.

Successful exploitation allows execution of arbitrary code when a user visits a malicious web site.

The vulnerability is reported in version 8.x. Other versions may also be affected.

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

References:

* BUGTRAQ: 20070403 ZDI-07-012: Yahoo! Messenger AudioConf ActiveX Control Buffer Overflow
http://www.securityfocus.com/archive/1/archive/1/464607/100/0/threaded

* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-07-012.html
* CONFIRM:
http://messenger.yahoo.com/security_update.php?id=031207
* CERT-VN: VU#388377
http://www.kb.cert.org/vuls/id/388377
* BID: 23291
http://www.securityfocus.com/bid/23291
* FRSIRT: ADV-2007-1219
http://www.frsirt.com/english/advisories/2007/1219
* SECTRACK: 1017867
http://www.securitytracker.com/id?1017867
* SECUNIA: 24742
http://secunia.com/advisories/24742
* NETVIGILANCE-UNKNOWN: 2523
http://securityreason.com/securityalert/2523
* XF: yahoo-yahooaudioconf-activex-bo(33408)
http://xforce.iss.net/xforce/xfdb/33408

CVE Reference: CVE-2007-1680

❖ 15560 Yahoo! Messenger Long Email Address Book Buffer Overflow (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

Rajesh Sethumadhavan has reported a vulnerability in Yahoo! Messenger, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the processing of address book entries and can be exploited to cause a buffer overflow when a user performs a mouse-over on a contact on the address book with an overly-long email address.

Successful exploitation allows execution of arbitrary code, but requires that the target user is e.g. tricked into accepting malicious contact details.

The vulnerability is reported in version 8.1. Other versions may also be affected.

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

References:

* FULLDISC: 20070716 Yahoo Messenger 8.1 Address Book Buffer Overflow
http://lists.grok.org.uk/pipermail/full-disclosure/2007-July/064669.html
* BID: 24926
http://www.securityfocus.com/bid/24926
* SECTRACK: 1018398
http://www.securitytracker.com/id?1018398
* SECUNIA: 26066
http://secunia.com/advisories/26066
* NETVIGILANCE-UNKNOWN: 2906
http://securityreason.com/securityalert/2906
* XF: yahoo-messenger-address-book-bo(35434)
http://xforce.iss.net/xforce/xfdb/35434

CVE Reference: CVE-2007-3928

❖ 15492 Yahoo! Messenger Webcam JPEG 2000 Processing Vulnerabilities (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

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.

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

References:

* MISC:
http://www.team509.com/expyahoo.rar
* MISC:
https://www.xfocus.net/bbs/index.php?act=ST&f=2&t=64639&page=1#entry321749
* MISC:
http://www.avertlabs.com/research/blog/index.php/2007/08/15/more-on-the-yahoo-messenger-webcam-0day/
* CERT-VN: VU#515968
http://www.kb.cert.org/vuls/id/515968
* BID: 25330
http://www.securityfocus.com/bid/25330
* FRSIRT: ADV-2007-2917
http://www.frsirt.com/english/advisories/2007/2917
* SECTRACK: 1018586
http://www.securitytracker.com/id?1018586
* SECUNIA: 26501
http://secunia.com/advisories/26501
* XF: yahoo-messenger-webcam-bo(36115)
http://xforce.iss.net/xforce/xfdb/36115

CVE Reference: CVE-2007-4391

❖ 15485 Yahoo! Widgets YDP ActiveX Control Buffer Overflow Vulnerability (Remote File Checking)

Parvez Anwar has discovered a vulnerability in Yahoo! Widgets, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the YDPCTL.YDPControl.1 (YDPCTL.dll) ActiveX control when handling the "GetComponentVersion()" method. This can be exploited to cause a stack-based buffer overflow by passing an overly long string (greater than 512 bytes) to the affected method.

Successful exploitation allows execution of arbitrary code.

The vulnerability is confirmed in YDPCTL.dll version 2007.4.13.1 included in Yahoo! Widgets version 4.0.3 (build 178). Other versions may also be affected.

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

References:

* CONFIRM:
http://help.yahoo.com/l/us/yahoo/widgets/security/security-08.html
* CERT-VN: VU#120760
http://www.kb.cert.org/vuls/id/120760
* BID: 25086
http://www.securityfocus.com/bid/25086
* FRSIRT: ADV-2007-2679
http://www.frsirt.com/english/advisories/2007/2679
* SECTRACK: 1018470
http://www.securitytracker.com/id?1018470
* SECUNIA: 26011
http://secunia.com/advisories/26011

CVE Reference: CVE-2007-4034

❖ 15439 Yahoo! Messenger YVerInfo.dll ActiveX Control Buffer Overflow (Remote File Checking)

Yahoo! Messenger is a free instant messaging software.

A vulnerability has been reported in Yahoo! Messenger, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the YVerInfo.dll ActiveX control and can be exploited to cause a buffer overflow e.g. when a user is tricked into viewing a malicious web page.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in YVerInfo.dll versions prior to 2007.8.27.1 included in Yahoo! Messenger downloaded before 2007-08-29.

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

References:

References:
* CONFIRM: 082907

http://messenger.yahoo.com/security_update.php?id=082907
* SECTRACK: 1018628
http://www.securitytracker.com/alerts/2007/Aug/1018628.html
* SECUNIA: 26579
http://secunia.com/advisories/26579/

CVE Reference: CVE-2007-4515

New Vulnerabilities found this Week

Yahoo! Messenger YVerInfo.dll ActiveX Control Buffer Overflow

"Execution of arbitrary code"

A vulnerability has been reported in Yahoo! Messenger, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the YVerInfo.dll ActiveX control and can be exploited to cause a buffer overflow e.g. when a user is tricked into viewing a malicious web page.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in YVerInfo.dll versions prior to 2007.8.27.1 included in Yahoo! Messenger downloaded before 2007-08-29.

References:
http://messenger.yahoo.com/download.php
http://descriptions.securescout.com/tc/15439

Novell Client NWSPOOL.DLL Buffer Overflow Vulnerabilities

"Crash; Execution of arbitrary code"

Secunia Research has discovered multiple vulnerabilities in Novell Client, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

The vulnerabilities are caused due to boundary errors within NWSPOOL.DLL when processing arguments passed to certain RPC requests (e.g. RpcAddPrinterDriver and RpcGetPrinterDriverDirectory). These can be exploited to cause stack-based buffer overflows via RPC requests with specially crafted, overly long arguments.

Successful exploitation allows crashing the service and execution of arbitrary code.

The vulnerabilities are confirmed in Novell Client v4.91 SP4 for Windows 2000/XP/2003. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2007-57/

Asterisk Voicemail IMAP Backend Invalid MIME Denial of Service

"Denial of Service"

A vulnerability has been reported in Asterisk, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error when handling emails with a malformed MIME body. This can be exploited to crash the service by sending a specially crafted email to a user and tricking him into listening to the voicemail.

Successful exploitation requires that the IMAP backend for the voicemail feature is used. Reportedly, other backends are not affected.

The vulnerability is reported in version 1.4.5 - 1.4.11. Other versions may also be affected.

References:
http://downloads.digium.com/pub/asa/AST-2007-021.html

Ipswitch WS_FTP Server Script Insertion Vulnerability

"Script insertion attacks"

John Harwold has discovered a vulnerability in Ipswitch WS_FTP Server, which can be exploited by malicious users to conduct script insertion attacks.

Parameters passed to valid FTP commands are not properly sanitized before the command is logged. This can be exploited to insert arbitrary HTML and script code, which is executed in the administrator's browser session in context of the administrative web interface when the malicious logs are viewed.

The vulnerability is confirmed in WS_FTP Server 6. Other versions may also be affected.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-August/065441.html

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