netVigilance

ScoutNews Team **20 August 2004**
Issue #34

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

It's a never ending cycle:
The first security flaws are found in XP SP2.
Auditors claim that US Homeland Security Department IT security lacks strategy.
The fourth amendment is used to challenge ID checks at airports and is expected to force employers to warn employees before monitoring mail in the future.
Phising set to grow as DIY kits are posted freely on the Internet.

Enjoy reading

Top Security News Stories this Week

❖ XP Service Pack 2: First security flaws found

"Microsoft never claimed that SP2 would close all the security holes"
Security researchers say they're starting to find flaws in Microsoft's latest major update for Windows XP.
Last week, German company Heise Security announced that two flaws could be used to circumvent the new warnings that Windows XP Service Pack 2, or SP2, normally would display about running untrusted programs, potentially giving a leg up to a would-be intruder's attempts to execute code on a victim's PC.
http://software.silicon.com/security/0,39024655,39123302,00.htm
Robert Lemos

❖ US security IT lacks strategy

The US government department responsible for dealing with terrorist threats has no appropriate strategy for managing its IT systems, say an official report.
The federal Department of Homeland Security (DHS) has no adequate blueprint to guide how it spends hundreds of millions of dollars on IT, according to US government auditors.
The blueprint, which the auditors say is "essential" in drawing up plans for information sharing to help the department counter terrorist threats, only provides a "partial basis" for running the IT systems as it is now out of date.
http://www.kablenet.com/kd.nsf/Frontpage/2E77E3FFEA1F368080256EF5003C2FE0?OpenDocument
Kablenet

❖ ID Checks at Airports Violate Fourth Amendment

EFF Protests Anti-Privacy Ruling in Appeal to the Ninth Circuit
California - US citizens may no longer have the right to travel without being searched. So says the District Court for the Northern District of California, which recently dismissed a case that questioned whether it is constitutional for airport security agents to demand identification papers from travelers. But the case, Gilmore v. Ashcroft, isn't going away. On Monday, counsel for plaintiff John Gilmore filed a brief with the Ninth Circuit, demanding that the court reverse this ruling and guarantee travelers the right to travel by air without the government requiring them to show identification papers.
http://www.eff.org/news/archives/2004_08.php#001833
Kurt Opshal

❖ **Do-it-yourself phishing kits found on the internet, reveals Sophos**

Sophos experts have discovered that do-it-yourself phishing kits are being made available for download free of charge from the internet.
Anyone surfing the web can now get their hands on these kits, launch their own phishing attack and potentially defraud computer users of the contents of their bank accounts.
These DIY kits contain all the graphics, web code and text required to construct bogus websites designed to have the same look-and-feel as legitimate online banking sites. They also include spamming software which enables potential fraudsters to send out hundreds of thousands of phishing emails as bait for potential victims.
http://www.sophos.com/spaminfo/articles/diyphishing.html
Sophos

❖ **Number crunching boffins unearth crypto flaws**

Cryptographic researchers have discovered weaknesses in the encryption algorithms that underpin the security and integrity of electronic signatures.
The issue concerns hash functions - one way mathematical functions that produce a small fixed length string from a much longer message. This is sometimes called a message digest. When two different input values produce the same output value this is called a collision. Teams of researchers have discovered collision in a series of hashing algorithms much more quickly than would be possible using brute-force attacks.
http://www.theregister.co.uk/2004/08/19/hash_crypto/
John Leyden

New Vulnerabilities Tested in SecureScout

➢ **14464 W32/Bagle.ad Worms**

This is a mass-mailing worm with the following characteristics:
- contains its own SMTP engine to construct outgoing messages
- harvests email addresses from the victim machine
- the From: address of messages is spoofed
- attachment can be a password-protected zip file, with the password included in the message body (as plaintext or within an image).
- contains a remote access component (notification is sent to hacker)
- copies itself to folders that have the phrase shar in the name (such as common peer-to-peer applications; KaZaa, Bearshare, Limewire, etc)
- uses various mutex names selected from those W32/Netsky variants have used, in order to prevent those W32/Netsky variants running on infected machines.
- the sample is packed with UPX runtime compressor.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=126562

- **14465 W32/Bagle.af Worms**
  This is a mass-mailing worm with the following characteristics:
  - contains its own SMTP engine to construct outgoing messages
  - harvests email addresses from the victim machine
  - the From: address of messages is spoofed
  - attachment can be a password-protected zip file, with the password included in the message body.
  - contains a remote access component (notification is sent to hacker)
  - copies itself to folders that have the phrase shar in the name (such as common peer-to-peer applications; KaZaa, Bearshare, Limewire, etc)
  - uses various mutex names selected from those W32/Netsky variants have used, in order to prevent those W32/Netsky variants running on infected machines
  - terminates processes of security programs and other worms
  - deletes registry entries of security programs and other worms

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=126792

- **14466 W32/Bagle.ai Worms**
  This is a mass-mailing worm with the following characteristics:
  - contains its own SMTP engine to construct outgoing messages
  - harvests email addresses from the victim machine
  - the From: address of messages is spoofed
  - attachment can be a password-protected zip file, with the password included in the message body.
  - contains a remote access component (notification is sent to hacker)
  - copies itself to folders that have the phrase shar in the name (such as common peer-to-peer applications; KaZaa, Bearshare, Limewire, etc)
  - uses various mutex names selected from those W32/Netsky variants have used, in order to prevent those W32/Netsky variants running on infected machines
  - terminates processes of security programs and other worms
  - deletes registry entries of security programs and other worms

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=126798

- **14467 W32/Mydoom.o Worm**
  This is a mass-mailing and share-hopping worm that bears the following characteristics:
  - mass-mailing worm constructing messages using its own SMTP engine
  - harvests email addresses from the victim machine

- spoofs the From: address
- contains a peer to peer propagation routine

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=127033

- **14468 W32/Mydoom.s Worm**

  This is a mass-mailing and share-hopping worm that bears the following characteristics:
  - mass-mailing worm constructing messages using its own SMTP engine
  - harvests email addresses from the victim machine
  - spoofs the From: address

  The virus arrives in an email message as follows:

  Subject : photos
  Body : LOL!;))))
  Attachment : photos_arc.exe

  When the attachment is run, the virus copies itself to the WINDOWS (%WinDir%) directory as rasor38a.dll, and to the SYSTEM (%SysDir%) directory as winpsd.exe.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=127616

- **19070 Adware CasinoOnNet**

  Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: L**ow**

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/c/casinoonnet.asp

- **19071 Adware CasinoRewards**

  Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/c/casinorewards.asp

- **19072 Adware Checkin**
  Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/c/checkin.asp

- **19073 Adware Claria**
  Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/c/claria.asp

- **19074 Adware ClickTheButton**
  Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/c/clickthebutton.asp

New Vulnerabilities found this Week

- **PHP-Fusion Public Accessible Database Backups**

"View sensitive data"

y3dips has reported a vulnerability in PHP-Fusion, allowing malicious people to view sensitive data.

1) Path information can be disclosed in error pages by passing invalid input or accessing scripts directly.

2) Database backup files are placed in a public accessible folder with easily guessable names. Backups are named using the date and time and is placed in

"fusion/fusion_admin/db_backups/".

This has been reported in PHP-Fusion 4.0.0 other versions may also be affected.

References: http://echo.or.id/adv/adv04-y3dips-2004.txt

❖ **MySQL "mysql_real_connect" Buffer Overflow Vulnerability**
"Buffer overflow and arbitrary code execution"

Lukasz Wojtow has reported a vulnerability in MySQL, potentially allowing malicious people to compromise a vulnerable system.

The problem is that the "mysql_real_connect()" function doesn't properly verify the length of IP addresses returned by a reverse DNS lookup of a hostname. This could potentially be exploited to cause a buffer overflow and execute arbitrary code.

Successful exploitation requires that the attacker is able to return a malicious DNS reply when a MySQL user connects to a server.

This has been reported in MySQL 4.0.20 and prior.

It has been reported that this can't be exploited on the Linux and OpenBSD platforms.

References: http://bugs.mysql.com/bug.php?id=4017

❖ **Qt BMP Handling Buffer Overflow Vulnerability**
"Heap-based buffer overflow"

Chris Evans has reported a vulnerability in the Qt library, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to boundary errors in the "read_dib()" function when handling 8-bit RLE encoded BMP files. This can be exploited by using an overly long length mark in order to cause a heap-based buffer overflow.

Successful exploitation may allow execution of arbitrary code and can be exploited via any application using the Qt library to display or decode BMP files.

NOTE: Some NULL pointer dereference errors within the handlers for XPM, GIF, and JPEG images can also be exploited to cause a DoS (Denial of Service).

The vulnerability affects version 3.3.2 and prior.

References: http://scary.beasts.org/security/CESA-2004-004.txt

❖ **Cisco IOS OSPF Packet Handling Denial of Service Vulnerability**
"Denial of Service"

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

The vulnerability is caused due to an error within the processing of OSPF packets. This can be exploited to cause an affected device to reload via a specially crafted OSPF packet.

The vulnerability affects Cisco IOS release trains based on 12.0S, 12.2, and 12.3.

Successful exploitation requires that OSPF protocol support has been enabled (not default setting).

References: http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml

❖ **Microsoft Internet Explorer Drag and Drop Vulnerability**
"Code execution"

http-equiv has discovered a vulnerability in Microsoft Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to insufficient validation of drag and drop events issued from the "Internet" zone to local resources. This can be exploited by a malicious website to e.g. plant an arbitrary executable file in a user's startup folder, which will get executed the next time Windows starts up.

http-equiv has posted a PoC (Proof of Concept), which plants a program in the startup directory when a user drags a program masqueraded as an image.

NOTE: Even though the PoC depends on the user performing a drag and drop event, it may potentially be rewritten to use a single click as user interaction instead.
References: http://secunia.com/advisories/9711/

❖ **YaPiG Arbitrary Command Execution Vulnerability**
"Execution of arbitrary PHP code"

aCiDBiTS has reported a vulnerability in YaPiG, which can be exploited by malicious people to compromise a vulnerable system.

User input passed to the "phid" parameter in "add_comment.php" is not properly verified before being used in a filename. This can be exploited to create a file with an arbitrary extension in a world-readable directory on the web server. The content of the file can be controlled due to insufficient input validation in "functions.php".

Successful exploitation may e.g. allow execution of arbitrary PHP code.

The vulnerability has been confirmed in version 0.92b. Other versions may also be affected.

References: http://secunia.com/advisories/12319/

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