netVigilance

ScoutNews Team **7 May 2004**
Issue #19

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Sasser, Sasser and Sasser, more versions expected to come over the next weeks, some voices are critical to Microsoft for their patch release policies asking if they are more marketing than security driven.
SecureScout was out with a test well in advance of the first Sasser variant and have added several more this week. Expect us to follow up as this saga continues.
As you may have noticed SecureScout has been adding adware test cases lately, now this area is being seen as the new nuisance area by others in the market – expect to see a bigger push in this area by SecureScout shortly.
New generations of wireless are expected to have better security out the box.

Enjoy reading

Top Security News Stories this Week

❖ Sasser infections hit Amex, others

Security experts are continuing to issue warnings about the Sasser Internet worm as organizations struggled to clean up the damage caused by infected hosts.
American Express Co. joined a number of U.S. universities in reporting infections from the Sasser worm on Monday and the SANS Institute's Internet Storm Center (ISC) maintained a yellow warning Tuesday despite expectations earlier in the day that the Sasser outbreak would wind down Monday, according to interviews.
http://www.infoworld.com/article/04/05/04/HNsasseramex_1.html?source=rss&url=http://www.infoworld.com/article/04/05/04/HNsasseramex_1.html
Paul Roberts

❖ Microsoft got off lightly with Sasser worm

I work in the Asia Pacific branch of one of the big 3 global IT outsourcers and I'd like to share an opinion on Sasser and this article in particular.
Microsoft has gotten off the hook with the media in regards to this issue quite nicely. To remind those that have forgotten: Several months back Microsoft switched from releasing security patches as were required to holding onto them and then releasing them in monthly installments. When do you want to feel secure? Now or later?

My take is that this move to release the patches in monthly installments is a PR exercise rather than one that is designed to help users and administrators. This was taken one step further in the latest round of patch releases where Microsoft bundled many fixes into just a few patches. These patches were essentially 'security rollup packs' or mini 'service packs'. When one patch changes so many things it increases the chances of the patch causing trouble with a given configuration. If a problem is found then the fixes for the - say - 8 vulnerabilities cannot be applied due to an issue with the fix for just one of them. How this new patch roll up system protects end users I can't quite understand.
http://www.theinquirer.net/?article=15756
The Letterman

❖ Sick of Spam? Prepare for Adware

The biggest threat to personal computing is neither spam nor viruses. Rather, it's the proliferation of a new category of deceptive software that takes over unwitting victims' computers for the purpose of gathering their personal information and bombarding them with unwanted advertising.
Dubbed spyware, adware, sneakware or malware -- depending on who you talk to -- these programs embed themselves deep inside a computer's operating system and spawn windows full of advertising messages, preventing users from accessing any other application. Or, they hide in the background, secretly transmitting information about the user's Web-surfing habits to a server somewhere on the Internet. If the user tries to delete the programs, they act like a cancer and replicate themselves over and over.
http://www.snpx.com/cgi-bin/news5.cgi?target=www.wired.com/news/technology/0,1282,63345,00.html?tw=rss.TEK
Amit Asaravala

❖ Countering Lack of Security in Wi-Fi Hot Spots

Public hotspots are not secure, not even turned on with Wired Equivalent Privacy (WEP), the 1999-era security standard of 802.11 Wi-Fi communications, making them a risk for any business professional to use, says Mike Disabato, senior analyst with the Burton Group.
In a report on "Securing the Mobile Device," Disabato outlines options that users tapping the 802.11 protocol have for securing their transmissions and guarding the integrity of their data.
http://www.wi-fiplanet.com/news/article.php/3348141
Bob Rudis

❖ Wi-Fi Security Improves

New standards will be certified and products shipping this year, say developers.
Two key improvements for the security and performance quality of Wi-Fi devices are scheduled to reach wireless network users this year as businesses and consumers continue to adopt wireless technology in greater numbers.
The Wi-Fi Alliance will certify products for the new 802.11i and 802.11e standards by September, says Frank Hanzlik, managing director of the Wi-Fi Alliance. The 802.11i standard is the complete version of the preliminary security standard WPA (Wi-Fi Protected Access) introduced last year, while 802.11e is a new standard that will improve the quality of wireless networks that transmit voice and video.
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/57946122?-2622
Tom Krazit

New Vulnerabilities Tested in SecureScout

- **14435 W32/Sasser.worm.a Worm (Registry Check)**

This worm:
Scans random IP addresses for exploitable systems.
Exploits the vulnerable system, by overflowing a buffer in LSASS.EXE.
Creates a remote shell on TCP port 9996.
Creates an FTP script named cmd.ftp on the remote host and executes it. This FTP script instructs the target victim to download and execute the worm (with the filename #_up.exe as aforementioned) from the infected host. The infected host accepts this FTP traffic on TCP port 5554.
Spawns multiple threads, some of which scan the local class A subnet, others the class B subnet, and others completely random subnets. The destination port is TCP 445

This self-executing worm spreads by exploiting a Microsoft Windows vulnerability [MS04-011 vulnerability (CAN-2003-0533)]

The worm spreads with the file name: avserve.exe
Unlike many recent worms, this virus does not spread via email. No user intervention is required to become infected or propagate the virus further. The worm works by instructing vulnerable systems to download and execute the viral code.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=125007

- **14436 W32/Sasser.worm.b & W32/Sasser.worm.c Worms (Registry Check)**

This worm:
Scans random IP addresses for exploitable systems.
Exploits the vulnerable system, by overflowing a buffer in LSASS.EXE.
Creates a remote shell on TCP port 9996.
Creates an FTP script named cmd.ftp on the remote host and executes it. This FTP script instructs the target victim to download and execute the worm (with the filename #_up.exe as aforementioned) from the infected host. The infected host accepts this FTP traffic on TCP port 5554.
Spawns multiple threads, some of which scan the local class A subnet, others the class B subnet, and others completely random subnets. The destination port is TCP 445

This self-executing worm spreads by exploiting a Microsoft Windows vulnerability [MS04-011 vulnerability (CAN-2003-0533)]

The worm spreads with the file name: avserve2.exe
Unlike many recent worms, this virus does not spread via email. No user intervention is required to become infected or propagate the virus further. The worm works by instructing

vulnerable systems to download and execute the viral code.

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=125008

- **14437 W32/Sasser.worm.d Worm (Registry Check)**

This worm:
Scans random IP addresses for exploitable systems.
Exploits the vulnerable system, by overflowing a buffer in LSASS.EXE.
Creates a remote shell on TCP port 9995.
Creates an FTP script named cmd.ftp on the remote host and executes it. This FTP script instructs the target victim to download and execute the worm (with the filename #_up.exe as aforementioned) from the infected host. The infected host accepts this FTP traffic on TCP port 5554.
Spawns multiple threads, some of which scan the local class A subnet, others the class B subnet, and others completely random subnets. The destination port is TCP 445

Unlike previous versions it functions with the following exceptions.

This variant spreads with the filename SKYNETAVE.EXE (16,384 bytes)
It sends ICMP echo packets to discover potential victims
It creates a remote shell on TCP Port 9995 rather than 9996

This self-executing worm spreads by exploiting a Microsoft Windows vulnerability [MS04-011 vulnerability (CAN-2003-0533)]

Unlike many recent worms, this virus does not spread via email. No user intervention is required to become infected or propagate the virus further. The worm works by instructing vulnerable systems to download and execute the viral code.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=125012

- **19039 Hijack Gigex SpeedDelivery**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/g/gigex_speeddelivery.asp

- **19040 Hijack GoHip**

Displays ads. Causes browser pop-ups. Hijacks browser settings. Tracks web usage. Collects personal info. Still live. Hard to remove.

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/g/gohip.asp

- **19041 Hijack HTMLEdit**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/h/htmledit.asp

- **19042 Hijack HungryHands**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/h/hungryhands.asp

- **19043 Hijack HuntBar**

HuntBar is a toolbar providing searching features, which is added to every new Internet Explorer and Windows Explorer window.

It also changes your home page and search bar settings to point to HuntBar's servers, and automatically opens this search bar when it detects you using any other search engine.

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/h/huntbar.asp

- **19044 Hijack I-Lookup**

ILookup is an IE toolbar which adds a search box and link buttons, bookmarks to the Favorites menu (mostly affiliate links) and hijacks both your home page and your Search sidebar. May track your browsing habits and report this info to a central ad server.

Alias: i-Lookup/GlobalWebSearch, ILookup, SearchBus (for I-Lookup/Sbus)

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/i/i-lookup.asp

New Vulnerabilities found this Week

Check Point VPN-1 ISAKMP Remote Buffer Overflow Vulnerability
It has been reported that Check Point VPN-1 products may be prone to a remote buffer overflow vulnerability that may allow a remote attacker to execute arbitrary code in order to gain unauthorized access.

The issue is reported to present itself in Check Point VPN-1 products during negotiations of a VPN tunnel. Specifically, a buffer overflow condition may be triggered by sending a malformed ISAKMP packet during the negotiations.

Check Point Software user who do not use Remote Access VPNs or gateway-to-gateway VPNs are not vulnerable to this issue.

Due to a lack of details, further information cannot be provided at the moment. This BID will be updated as more information becomes available.

For more information, see :
http://www.securityfocus.com/bid/10273/discussion/

Linux Kernel Panic Function Call Undisclosed Buffer Overflow Vulnerability
The panic() function call of the Linux kernel has been reported prone to a buffer overflow vulnerability. The exact details of the overflow are currently unspecified, however it has been reported that this issue cannot be exploited. Other reports suggest that the issue may be exploited to reveal portions of kernel memory space.
http://www.securityfocus.com/bid/10233
Linux Kernel Setsockopt MCAST_MSFILTER Integer Overflow Vulnerability

An integer overflow vulnerability has been reported in the setsockopt() system call. This was introduced as of the 2.4.22/2.6.1 kernel releases.

The specific issue exists in the net/ipv4/ip_sockglue.c source file and is present in the ip_setsockopt() subroutine of the setsockopt() system call. Within this subroutine there is an integer overflow within the IP_MSFILTER_SIZE macro, which is used when setting the MCAST_MSFILTER socket option.

This issue may be exploited by a local user to compromise the system. Exploitation could also result in a denial of service. It should be noted that this type of vulnerability may provide a generic means of privilege escalation across Linux distributions once a remote attacker has gained unauthorized access as a lower privileged user.

For more information, see :
http://www.securityfocus.com/bid/10179

Linux kernel do_fork() Memory Leakage Vulnerability
It has been reported that the Linux kernel may be prone to a memory leakage vulnerability. The issue exists because memory is allocate for child processes but never freed.

This issue has been identified in kernel versions 2.4 and 2.6.

For more information, see :
http://www.securityfocus.com/bid/10221/discussion/

Apache Mod_SSL HTTP Request Remote Denial Of Service Vulnerability
mod_ssl has been reported to be prone to a remote denial of service vulnerability. It has been

reported that the issue is as a result of a memory leak and will present itself when standard HTTP requests are handled on the SSL port of an affected Apache server.

For more information, see :
http://www.securityfocus.com/bid/9826/discussion/

Apache Error Log Escape Sequence Injection Vulnerability
It has been reported that the Apache web server is prone to a remote error log escape sequence injection vulnerability. This issue is due to an input validation error that may allow escape character sequences to be injected into apache log files.

This may facilitate exploitation of issues such as those found in BIDs 6936 and 6938.

This issue may allow an attacker to carry out a number of actions including arbitrary file creation and code execution on the affected system.

For more information, see :
http://www.securityfocus.com/bid/9930/discussion/

Business Objects Crystal Reports Multiple Unspecified Vulnerabilities
It has been reported that Crystal Reports may be prone to multiple vulnerabilities in the web interface supplied with the application. These issues could allow an attacker to disclose or delete files from a server running the application as well as cause a denial of service condition.

Crystal Reports versions 10.0 and prior are assumed to be vulnerable to these issues.

Due to a lack of details further information is not available at the moment. This BID will be updated as more information becomes available.

For more information, see :
http://www.securityfocus.com/bid/10260/discussion/

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