netVigilance

ScoutNews Team

14 May 2004
Issue #20

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Sasser for the fifth time and a parasite worm to Sasser – yes, it continues even with the original Sasser author in jail. SecureScout is proving to be a unique tool for you to control your environment with.
More work is being done from both chip and operating system companies to arrest security issues already from the birth of new technology generations. This both for wire based and wire less connections.

Enjoy reading

Top Security News Stories this Week

➢ **Fifth Sasser 'released before arrest'**
The latest variant of the worm contains a warning to unpatched PCs that they are vulnerable to attack
Antivirus companies discovered a fifth version of the Sasser variant this weekend, within hours of German police arresting an 18-year-old man who confessed to being the Sasser worm's author.
The latest variant, Sasser.E, was released a week ago, according to Microsoft. It attempts to warn people whose computers are vulnerable that their systems have not been patched for a widespread Microsoft Windows vulnerability exploited by the program.
http://news.zdnet.co.uk/business/0,39020645,39154256,00.htm

➢ **Security and 64-bits coming to Intel's Prescott in June**
Later this year, Intel Corp. will turn on security features and 64-bit extensions within the Prescott core as it ships PC and server processors based on Prescott and the Grantsdale chipset in the second half of the year, Intel President and Chief Operating Officer Paul Otellini said during Intel's spring analyst meeting Thursday in New York.
Prescott supports the NX (no execute) feature that will prevent worms and viruses from executing dangerous code through the exploitation of buffer overflows, Otellini said during a Webcast of the event. Advanced Micro Devices Inc.'s Athlon 64 and Opteron processors also come with this feature, which requires software support from Microsoft Corp.'s Windows XP Service Pack 2 expected later this year.
http://www.infoworld.com/article/04/05/13/HNprescott_1.html

➢ **Symantec, Norton need vital patches in next 24 hours**

Almost the entire range of Symantec Corp. security software, from Norton Internet Security through to the Symantec Firewall require urgent updates, the company has warned, after a series of four extremely critical vulnerabilities were found by security company eEye Digital Security Inc.

One of the holes remains open even with all ports filtered and intrusion rules set thanks to a separate design flaw, eEye has warned. This makes it an almost certain target for worm writers, one of which -- if history is to be believed -- may be put out on the Net within 24 hours.

http://www.infoworld.com/article/04/05/13/HNvitalpatches_1.html

➢ **Security threats raise concerns about Bluetooth**

Potential security risks posed by the Bluetooth wireless technology are prompting some IT managers to rein in use of Bluetooth-equipped mobile phones and PCs on their networks. Bluetooth vendors are scheduled to hold a press briefing today at which they will discuss the security issues and provide guidance on how users can guard their devices against hackers. But several IT managers last week said they now see a need to protect their networks from Bluetooth attacks by taking the same steps they took to secure their corporate wireless LANs.

http://www.infoworld.com/article/04/05/10/HNbluetooth_1.html

➢ **Search engines delete adware company**

Yahoo and Google have disabled links to controversial adware maker WhenU after the company was accused of engaging in unauthorized practices aimed at boosting its search rankings, WhenU's top executive confirmed Thursday.

The practices came to light following an investigation by antispyware crusader Ben Edelman, a Harvard student who found that the company used a technique known as "cloaking" to dupe search engines into favorably listing decoy Web pages that direct people to other destinations, once they click on the link.

http://news.com.com/2100-1024_3-5212479.html?part=rss&tag=feed&subj=news

➢ **Netsky falls**

FIVE GERMAN GEEKS are now helping police with their inquiries into the Netsky virus ring.

Since the arrest, police have raided the homes of five youths who are believed to be in the Netsky ring. Their computers have been taken away for questioning too.

http://www.theinquirer.net/?article=15895

➢ **Windows XP Service Pack 2: What you'll get and when you'll get it**

A look at Gates and co's latest security baby

Microsoft has been showing off its Service Pack 2 offering and dropping some serious hints as to what users can expect from the security-focused, soon-to-be-ubiquitous offering.

The message from the Redmond types is that SP2 is not just a collection of patches, it's a more comprehensive addition of security code as well as other software bits and bobs – like an overhaul of the wireless LAN user interface – that will turn up on users' desktops as well.

http://software.silicon.com/os/0,39024651,39120655,00.htm

➢ **Spec in Works to Secure Wireless Networks**

The Trusted Computing Group said Monday that it is working on a specification to ensure that wireless clients connecting to a network won't serve as a back door to worms and crackers.

Officials within the TCG, based in Portland, Ore., said the industry standards body is developing a "Trusted Network Connect" specification, designed to audit wireless-enabled

PCs when they first make contact with an enterprise's wireless network.
http://www.eweek.com/article2/0,1759,1590243,00.asp

New Vulnerabilities Tested in SecureScout

- **14396 Cumulative Security Update for Internet Explorer (MS04-004/832894)**

This is a cumulative update that includes the functionality of all the previously-released updates for Internet Explorer 5.01, Internet Explorer 5.5, and Internet Explorer 6.0. Additionally, it eliminates the following three newly-discovered vulnerabilities:

A vulnerability that involves the cross-domain security model of Internet Explorer.
A vulnerability that involves performing a drag-and-drop operation with function pointers during dynamic HTML (DHTML) events in Internet Explorer.
A vulnerability that involves the incorrect parsing of URLs that contain special characters.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gain Root** Risk: **High**

CVE Links: CAN-2003-1026; CAN-2003-1027; CAN-2003-1025

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-004.mspx

- **14439 Vulnerability in Help and Support Center Could Allow Remote Code Execution (MS04-015/840374)**

This update resolves a newly-discovered vulnerability. A remote code execution vulnerability exists in the Help and Support Center because of the way that it handles HCP URL validation. The vulnerability is documented in the Vulnerability Details section of this bulletin.

If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

CVE Links: CAN-2004-0199

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-015.mspx

- **14440 W32/Sasser.worm.e 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 1022.

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 1023.
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
Attempts to disable Bagle variants by removing registry keys created by Bagle

Unlike previous versions it functions with the following exceptions.

This variant spreads with the filename lsasss.exe (15,872)

This self-executing worm spread 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=125091

- **14441 W32/Sasser.worm.f 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 Link: GENERIC-MAP-NOMATCH

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=125095

- **19045 Adware AdvSearch**

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/advsearch.asp

- **19046 Adware Adware.IEPageHelper**

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/adware_iepagehelper.asp

- **19047 Adware ArmBender**

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/armbender.asp

- **19048 Adware AtHoc**

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

Toolbar: A group of buttons which perform common tasks. A toolbar for Internet Explorer is nomally located below the menu bar at the top of the form. Toolbars may be created by Browser Helper Objects.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/athoc.asp

- **19049 Adware Atztecmarketing.syscpy**

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

Toolbar: A group of buttons which perform common tasks. A toolbar for Internet Explorer is nomally located below the menu bar at the top of the form. Toolbars may be created by Browser Helper Objects.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/atztecmarketing_syscpy.asp

- **19050 Adware Aureate Group Mail**

Aureate Group Mail is an email application designed specifically for Mailing List management and Distribution. If you maintain mailing lists or if you regularly send messages to large groups of recipients, then Aureate Group Mail will be your saviour. Aureate Group Mail is perfect for keeping friends, customers, investors, and clients digitally informed.

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/aureate_group_mail.asp

- **19051 Adware BargainBuddy**

BargainBuddy is a Browser Helper Object that watches the pages your browser requests and the terms you enter into a search engine web form. If a term matches a preset list of sites or keywords, BargainBuddy will display an ad. A process that is invoked at machine startup will check a remote server for updates to the software and ads that will be displayed.Bargain Buddy consists of an IE Browser Helper Object, and a process set to run at startup. The BHO monitors web pages requested and terms entered into forms. If there is a match with a preset list of sites and keywords, an advertisement may be shown. The process can contact its maker's server to download updates to the list of adverts and to the software itself.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/b/bargainbuddy.asp

New Vulnerabilities found this Week

Dabber exploits Sasser flaw
Virus writers have created a worm that exploits coding flaws in the infamous Sasser worm to spread.
Dabber uses a flaw in the FTP server component of the Sasser worm. The worm will only infect users already infected by Sasser, according to security services firm LURHQ. "Even though we have seen worms utilize backdoors left behind by other worms, this is the first time we have seen a worm using a vulnerability in another worm in order to propagate," it said.
http://www.theregister.co.uk/2004/05/14/dabber_worm/

Security holes uncovered in Symantec, Norton products
Almost the entire range of Symantec Corp. security software, from Norton Internet Security through to the Symantec Firewall, requires urgent updates, the company has warned, after four critical vulnerabilities were found.
http://www.computerworld.com/securitytopics/security/holes/story/0,10801,93120,00.html?f=x10

Microsoft Outlook Mail Client E-mail Address Verification Weakness
It has been reported that Microsoft Outlook mail client may be prone to a weakness that could allow a remote attacker to verify the validity of a recipient's e-mail address. This issue may result in a victim receiving more junk e-mail.

Microsoft Outlook 2003 is reported to be affected by this issue.
http://www.securityfocus.com/bid/10323/discussion/

Exim Sender Verification Remote Stack Buffer Overrun Vulnerability
Exim has been reported prone to a remotely exploitable stack-based buffer overrun vulnerability.

This is exposed if sender verification has been enabled in the agent and may be triggered by a malicious e-mail. Exploitation may permit execution of arbitrary code in the content of the mail transfer agent.
http://www.securityfocus.com/bid/10290/info/

Exim Header Syntax Checking Remote Stack Buffer Overrun Vulnerability
Exim is reportedly prone to a remotely exploitable stack-based buffer overrun vulnerability.

This issue is exposed if header syntax checking has been enabled in the agent and may be triggered by a malicious e-mail. Though not confirmed to be exploitable, if this condition were to be exploited, it would result in execution of arbitrary code in the context of the mail transfer agent. Otherwise, the agent would crash when handling malformed syntax in an e-mail message.
http://www.securityfocus.com/bid/10291

RSync Configured Module Path Escaping Vulnerability

If an rsync server is installed as a daemon with a read/write enabled module without using the 'chroot' option, it is possible that a remote attacker could write files outside of the configure module path. Rsync does not properly sanitize the paths when not running with chroot.

The result is that attackers may potentially write files to the system, resulting in various consequences such as execution of arbitrary code or denial of service.

http://www.securityfocus.com/bid/10247

Samba SMB/CIFS Packet Assembling Buffer Overflow Vulnerability

A buffer overflow vulnerability has been reported for Samba. The vulnerability occurs when the smbd service attempts to re-assemble specially crafted SMB/CIFS packets.

An attacker can exploit this vulnerability by creating a specially formatted SMB/CIFS packet and send it to a vulnerable Samba server. The overflow condition will be triggered and will result in smbd overwriting sensitive areas of memory with attacker-supplied values.
http://www.securityfocus.com/bid/7106

Microsoft Internet Explorer Unconfirmed Memory Corruption Vulnerability

It has been reported that Internet Explorer may be prone to a potential memory corruption vulnerability that could allow a remote attacker to cause a denial of service condition in the browser. The issue is reported to present itself when an attacker creates a malicious site, which employs the 'onLoad' event and the 'window.location' javascript method to access a local file.
http://www.securityfocus.com/bid/10299

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.

http://www.securityfocus.com/bid/9826

EMule Web Control Panel Denial Of Service Vulnerability

It has been reported that eMule's Web Control Panel is susceptible to a remote denial of service vulnerability.

This issue is reportedly triggered by sending malformed requests to the web interface. Upon processing malformed requests, the affected application will crash, denying service to legitimate users.

http://www.securityfocus.com/bid/10317

Microsoft Internet Explorer XML Parsing Denial Of Service Vulnerability

Internet Explorer is reportedly affected by a XML parsing denial of service vulnerability. This issue is due to a failure of the application to properly handle malformed XML tags.

Successful exploitation of this issue might allow a remote attacker to crash a vulnerable web browser.

http://www.securityfocus.com/bid/10318

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