netVigilance

ScoutNews Team **19 June 2004**
Issue #25

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Wireless and IP telephony seem to be the next two technologies to add big security issues.

There is a new Phishing Index in town.

A spammer settles a suit and a worm writer admits it was for fame as he is looking for a real job.

Enjoy reading

Top Security News Stories this Week

- **Wireless LANs are the major wireless security problem, says Gartner**

Until 2006, 70% of successful wireless local area network (WLAN) attacks will be because of the misconfiguration of WLAN access points (AP) and client software, according to Gartner. Security for WLANs and personal digital assistants (PDAs) in the company needs to be driven by updated security policies that address the unique demands of the mobile workplace.
http://www.internetworld.co.uk/WLAN/Article35395.aspx
George Malim

- **IP phones can create network security risk**

The increasing adoption of Internet telephony may be opening up a significant security risk for companies
While mobile telephone viruses have been the subject of headlines recently, IP-based telephones could represent a more immediate security threat for many businesses. "Attacks on IP phones are actually quite frequent," said Roy Wakim, convergence solutions manager at Avaya South Pacific. "Security is a major issue."
http://news.zdnet.co.uk/communications/networks/0,39020345,39158003,00.htm
Angus Kidman

- **Computer virus writer: "Netsky worm made me the hero of my class"**

An interview with German teenager Sven Jaschan, arrested in connection with the

Sasser and Netsky virus outbreaks, has revealed that all of his classmates at college knew that he was the author of the destructive worms.
http://www.sophos.com/virusinfo/articles/netskyhero.html
Sophus

❖ **Security Vendor Launches Phishing Index**

Message security vendor MailFrontier on Thursday launched the Phishing Index, a score that tracks users' current overall vulnerability to phishing attacks.
The index takes multiple factors into consideration and is a "compilation of an exhaustive evaluation of thousands of phishing e-mails and how people interact with those messages," the Palo Alto, Calif.-based vendor claimed.
http://www.techweb.com/wire/story/TWB20040617S0002
TechWebNews

❖ **Canadian spammer sued by Yahoo, Sophos reports**

Twenty-five-year-old Eric Head from Kitchener, near Toronto in Canada, has been accused of being one of the world's most prolific spammers, sending an alleged 94 million spams in just one month, according to media reports.
In March, the global internet provider Yahoo sued Head, along with his father and brother, for sending spam. This lawsuit is part of an industry crackdown on hundreds of people who are filling email users inboxes with unwanted spam.
Head is reported to having agreed to paying in excess of US $100,000 to Yahoo as part of his settlement.
http://www.sophos.com/spaminfo/articles/canadian_spammer.html
Sophus

New Vulnerabilities Tested in SecureScout

➢ **14040 Windows User Account has UserName as Password Vulnerability**

A Windows NT domain user or administrator account has a password defined as his account username.

Note that if a network drive is mapped between the engine and the tested target, or another connection already exists the test result will be unknown.

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

CVE Links: CAN-1999-0506

Reference: http://support.microsoft.com/support/kb/articles/q161/9/90.asp & http://support.microsoft.com/default.aspx?scid=kb;en-us;Q225230 & http://www.sans.org/top20/#W3

➢ **14209 Active Sessions Enumeration is possible**

A listing of active sessions on the target host could be retrieved. This will display all resources which are currently being accessed on the target host.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: NA

➢ 14234 Multiples Vulnerabilities in Handling URLs with Internet Explorer (MS01-051/Q306121)

Three vulnerabilities affect Internet Explorer:
Zone Spoofing vulnerability, HTTP Request Encoding vulnerability, New variant of Telnet Invocation vulnerability.

The first involves how IE handles URLs that include IP addresses containing any dot. When a malformed request using an IP format without any dot is made, IE would treat the site as an intranet site, and open pages on the site in the Intranet Zone rather than the correct zone.

The second involves how IE handles URLs that specify third-party sites. By encoding an URL in a particular way, it would be possible for an attacker to include HTTP requests that would be sent to the site as soon as a connection had been established. That allows it attackers to take action on the user's behalf, including sending a request to delete data.

The third is a new variant of a vulnerability discussed in Microsoft Security Bulletin MS01-015, affecting how Telnet sessions are invoked via IE.
The flaw does not lie in the Telnet client, but in IE, which should not allow Telnet to be started remotely with command-line arguments.

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

CVE Link: CVE-2001-0664 & CVE-2001-0665 & CVE-2001-0667

Reference: http://www.microsoft.com/technet/security/bulletin/MS01-051.mspx & http://www.securityfocus.com/bid/3420 & http://www.securityfocus.com/bid/3421

➢ 14452 Symantec Norton AntiVirus - Virus Definitions Outdated

Virus signatures are used to detect and repair the most recently discovered viruses.

Your definitions are older than 30 days which means that you might be vulnerable to current viruses.

See References for a list of current viruses.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.sarc.com/

➢ 15488 Cisco CatOS Telnet, HTTP and SSH Vulnerability

A TCP-ACK DoS attack is conducted by not sending the regular final ACK required for a 3-way TCP handshake to complete, and instead sending an invalid response to move the connection to an invalid TCP state. This attack can be initiated from a remote spoofed source.

This vulnerability is currently known to be exploitable only if you have the Telnet, HTTP or SSH service configured on a device which is running Cisco CatOS.

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

CVE Link: CAN-2004-0551

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20040609-catos.shtml & http://www.securityfocus.com/bid/10504

- **17710 Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (MS03-051/813360)**

This bulletin addresses two new security vulnerabilities in Microsoft FrontPage Server Extensions, the most serious of which could enable an attacker to run arbitrary code on a user's system.

The first vulnerability exists because of a buffer overrun in the remote debug functionality of FrontPage Server Extensions. This functionality enables users to remotely connect to a server running FrontPage Server Extensions and remotely debug content using, for example, Visual Interdev. An attacker who successfully exploited this vulnerability could be able to run code with IWAM_machinename account privileges on an affected system, or could cause FrontPage Server Extensions to fail.

The second vulnerability is a Denial of Service vulnerability that exists in the SmartHTML interpreter. This functionality is made up of a variety of dynamic link library files, and exists to support certain types of dynamic web content. An attacker who successfully exploited this vulnerability could cause a server running Front Page Server Extensions to temporarily stop responding to requests.

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

CVE Link: CAN-2003-0822 & CAN-2003-0824

Reference: http://www.microsoft.com/technet/security/bulletin/MS03-051.mspx

- **17709 Vulnerability in Crystal Reports Web Viewer Could Allow Information Disclosure and Denial of Service (MS04-017/842689) (DoS)**

This update resolves a newly-discovered vulnerability in Crystal Reports and Crystal Enterprise from Business Objects. Microsoft Visual Studio .NET 2003 (all versions) and Outlook 2003 with Business Contact Manager redistribute Crystal Reports and are therefore affected by the vulnerability. Microsoft Business Solutions CRM 1.2 redistributes Crystal Enterprise, which is affected in the same way.

An attacker who successfully exploited the vulnerability could retrieve and delete files through the Crystal Reports and Crystal Enterprise Web viewers on an affected system. The number of files of files that are impacted by this vulnerability would depend on the security context of the affected component that is used by the Crystal Web viewer.

Note that Systems can only be vulnerable if they have Internet Information Services (IIS) installed.

Once the target is found to be vulnerable, the file %installdir%\system32\drivers\etc\lmhosts.sam is deleted. Therefore this vulnerability can not be reproduced successfully twice.

The vulnerabiliy can only be found if the user used by the ASP.NET has the proper access rights to the "[WIN_DIR]/system32/drivers/etc/" directory.

By default directory is secure except if partition is fat32.

Test Case Impact: **DoS** Vulnerability Impact: **DoS** Risk: **Medium**

CVE Link: CAN-2004-0204

Reference: http://www.microsoft.com/technet/security/bulletin/ms04-017.mspx

➢ 17900 Linksys Router DoS Vulnerability

Linksys is known as the leader in networking solutions for the home and small business particularly wireless LAN equipment, broadband routers, network adapters for the desktop and notebook PC and hubs and switches.

Linksys router provide an HTTP remote management interface.

It is possible to deny the http service of the router with specific craft URL.

Test Case Impact: **DoS** Vulnerability Impact: **DoS** Risk: **Medium**

CVE Link: GENERIC-MAP-NOMATCH

Reference: www.linksys.com

➢ 17901 Linksys remote HTTP management access Vulnerability

Linksys is known as the leader in networking solutions for the home and small business particularly wireless LAN equipment, broadband routers, network adapters for the desktop and notebook PC and hubs and switches.

Linksys router provide an HTTP remote management interface.

It has been reported than even if the Remote management option is disable, the HTTP and HTTPS remote management ports are still reachable on the WAN interface.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: www.linksys.com

New Vulnerabilities found this Week

- **Cisco IOS BGP Processing Denial of Service Vulnerability**

« extended DOS attack »

The Border Gateway Protocol (BGP) is a routing protocol defined by RFC 1771, and designed to manage IP routing in large networks. An affected Cisco device running a vulnerable version of Cisco IOS software and enabling the BGP protocol will reload when a malformed BGP packet is received. BGP runs over TCP, a reliable transport protocol which requires a valid three way handshake before any further messages will be accepted. The Cisco IOS implementation of BGP requires the explicit definition of a neighbor before a connection can be established, and traffic must appear to come from that neighbor. These implementation details make it very difficult to send a BGP packet to a Cisco IOS device from an unauthorized source.

A Cisco device receiving an invalid BGP packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack. This issue is documented in bug IDs CSCdu53656 (registered customers only) and CSCea28131 (registered customers only) .

References:http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml

- **Internet Explorer File Download Error Message Denial of Service Weakness**

« crash a user's browser »

Rafel Ivgi has discovered a weakness in Internet Explorer (IE), allowing malicious people to crash a user's browser.

Analysis indicates that the issue is caused due to an error during the construction of a file download error message dialog box like the following:

"Internet Explorer cannot download [file] from [server]"

It is possible to trigger the issue via a specially crafted link like:
Link

This causes an incorrect pointer to be passed as argument in a call to "_snwprintf()" instead of the correct pointer to the string: "[file] from [server]". This may result in an access violation, if the pointer refers to an inaccessible memory location, which varies depending on the supplied value after the "%" character.

The problem has been confirmed on a fully patched system with IE 6.0. Other versions may also be affected.

Successful exploitation crashes the browser, if a user is tricked into right clicking the link and choosing "Save Target As...". It is currently not believed that this issue can be exploited for code execution purposes.

References:http://secunia.com/advisories/11868/

❖ **Linux Kernel "__clear_fpu()" Macro Denial of Service Vulnerability**
« crash the kernel »

Stian Skjelstad has reported a vulnerability in the Linux kernel allowing malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the "__clear_fpu()" macro and can be exploited to crash the kernel via a specially crafted program containing assembler inlines, which manipulate the floating-point state.

References: http://linuxreviews.org/news/2004-06-11_kernel_crash/index.html

❖ **PHP-Nuke Multiple Vulnerabilities**
« cross-site scripting attacks, disclose path information, cause a DoS »

Janek Vind has reported multiple vulnerabilities in PHP-Nuke, which can be exploited by malicious people to conduct cross-site scripting attacks, disclose path information, and cause a DoS (Denial of Service).

1) Input passed to various parameters in the "Reviews", "Encyclopedia", and "Faq" modules isn't properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

2) An input validation error within the "Reviews" module can be exploited to manipulate SQL queries by passing arbitrary SQL code to the "order" parameter.

3) Path information can be disclosed in error pages by passing invalid input to the "preview_review()" function in the "Reviews" module.

4) An input validation error within the score subsystem of the "Reviews" module can be exploited to manipulate scores, disclose path information, and ultimately cause the server to consume excessive amounts of CPU and memory resources.

The vulnerabilities have been reported in versions 6.x through 7.3.

References: http://www.waraxe.us/index.php?modname=sa&id=32

❖ **HP-UX ftp Pipe Character Arbitrary Command Execution Vulnerability**
« execute arbitrary commands »

HP has acknowledged a very old vulnerability in ftp for HP-UX, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an input validation error in the ftp client when handling filenames. This can be exploited to execute arbitrary commands on a user's system via a file with a specially crafted filename beginning with a pipe character ("|").

Successful exploitation requires that a user is tricked into retrieving a malicious file.

The vulnerability affects HP-UX B.11.00, B.11.11, and B.11.22.

References: http://www.kb.cert.org/vuls/id/258721

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