netVigilance

ScoutNews Team **14 June 2004**
Issue #24

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Cisco and Trend Micro team to offer protection against worms in Cisco gear, as Cisco Systems low end gear from Linksys has a hole that opens up to households.

More vulnerability in Microsoft Internet Explorer as well as tool used in most open source products.

Red Hat team up with Intel Architecture chip vendors to halt worm and virus spreading at the lower level of its Linux operating system

Enjoy reading

Top Security News Stories this Week

❖ Trend Micro, Cisco to fight worms

Cisco Systems Inc. and Trend Micro Inc. announced a partnership under which Cisco will improve its routers, switches and firewalls with Trend's worm-blocking technology.
Trend Micro, which uses the technology in its own VirusWall product, plans to make its signature-based worm-blocking technologies available in Cisco products by the third quarter.
Cisco says the technology initially will fit into its intrusion-detection code base and be used to stop network worms that take advantage of software vulnerabilities. Trend Micro will supply updates, which will be managed via CiscoWorks and other Cisco management tools.
http://www.infoworld.com/article/04/06/08/HNtrendcisco_1.html
Ellen Messmer

❖ New Internet Explorer holes causing alarm

Four new holes have been discovered in the Internet Explorer (IE) Web browser that could allow malicious hackers to run attack code on Windows systems, even if those systems have installed the latest software patches from Microsoft Corp., security experts warned.
Some of the flaws are already being used to attack Windows users and include a glitch that allows attackers to fake or "spoof" the address of a Web page, as well as vulnerabilities that enable malicious pages from the Internet to be handled by IE with very little scrutiny or security precautions.
http://www.computerworld.com/securitytopics/security/holes/story/0,10801,93803,00.html?f

=x10
Paul Robberst

❖ Security holes splatter Open Source

A KEY OPEN source tool used by developers to track and manage changes in computer code has six security glitches and counting.
Concurrent Versions System (CVS) is used to manage code on a number of top open source software development projects.
Discovered by German security firm E-matters, the six holes could enable remote attackers to launch denial of service attacks or run malicious code on systems hosting vulnerable versions of CVS.
http://www.theinquirer.net/?article=16524
Nick Farrell

❖ Linksys flaw opens door to home networks

Cisco Systems has issued a patch for a security flaw in one of its Linksys routers that could give hackers access to consumers' home networks.
Alan Rateliff II, an independent security consultant, on Friday said he discovered a vulnerability in the Linksys WRTS54G 802.11g wireless router. The flaw gives hackers a free pass into the Web-based configuration page of the router when the firewall function is turned off.
http://www.zone-h.org/en/news/read/id=4270
Marguerite Reardon

❖ Linux gains virus armour

Linux seller Red Hat and chipmaker Intel released prototype Linux software this week to support a security technology designed to curtail the spread of viruses.
The security technology, called NX for "no execute," is built into several "x86" processors from Intel, AMD and Transmeta. The technology is designed to block vulnerabilities that viruses and worms use to spread, but operating system support is required for NX to work.
http://www.zone-h.org/en/news/read/id=4269
Stephen Shankland

New Vulnerabilities Tested in SecureScout

➢ 14445 Vulnerability in DirectPlay Could Allow Denial of Service (MS04-016/839643)

This update resolves a newly-discovered, privately reported vulnerability. A denial of service vulnerability exists in the implementation of the IDirectPlay4 application programming interface (API) of Microsoft DirectPlay because of a lack of robust packet validation. The vulnerability is documented in the Vulnerability Details section of this bulletin.

If a user is running a networked DirectPlay application, an attacker who successfully exploited this vulnerability could cause the DirectPlay application to fail. The user would have to restart the application to resume functionality.

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

CVE Links: CAN-2004-0202

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-016.mspx

- **14447** Flaw in Microsoft Word Could Enable Macros to Run Automatically (MS03-035/827653)

A macro is a series of commands and instructions that can be grouped together as a single command to accomplish a task automatically. Microsoft Word supports the use of macros to allow the automation of commonly performed tasks. Since macros are executable code it is possible to misuse them, so Microsoft Word has a security model designed to validate whether a macro should be allowed to execute depending on the level of macro security the user has chosen.

A vulnerability exists because it is possible for an attacker to craft a malicious document that will bypass the macro security model. If the document was opened, this flaw could allow a malicious macro embedded in the document to be executed automatically, regardless of the level at which macro security is set. The malicious macro could take the same actions that the user had permissions to carry out, such as adding, changing or deleting data or files, communicating with a web site or formatting the hard drive.

The vulnerability could only be exploited by an attacker who persuaded a user to open a malicious document -there is no way for an attacker to force a malicious document to be opened.

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

CVE Links: CAN-2003-0664 & CAN-1999-0354

Reference: http://www.microsoft.com/technet/security/bulletin/ms03-035.mspx &
http://www.microsoft.com/technet/security/bulletin/ms99-002.mspx &
http://www.sans.org/top20/#W8

- **14448 E-mail Editor Flaw Could Lead to Script Execution on Reply or Forward (MS02-021/Q321804)**

Outlook 2000 and 2002 provide the option to use Microsoft Word as the e-mail editor when creating and editing e-mail in either Rich-Text or HTML format. A security vulnerability exists when Outlook is configured this way and the user forwards or replies to a mail from an attacker.

The vulnerability results from a difference in the security settings that are applied when displaying a mail versus editing one. When Outlook displays an HTML e-mail, it applies Internet Explorer security zone settings that disallow scripts from being run. However, if the user replies to or forwards a mail message and has selected Word as the e-mail editor, Outlook opens the mail and puts the Word editor into a mode for creating e-mail messages. Scripts are not blocked in this mode.

An attacker could exploit this vulnerability by sending a specially malformed HTML e-mail containing a script to an Outlook user who has Word enabled as the e-mail editor. If the user replied to or forwarded the e-mail, the script would then run, and be capable of taking any action the user could take.

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

CVE Link: CVE-2002-1056

Reference: http://www.microsoft.com/technet/security/bulletin/ms02-021.mspx & http://www.sans.org/top20/#W8

- **14449 Outlook View Control Exposes Unsafe Functionality (MS01-038)**

The Microsoft Outlook View Control is an ActiveX control that allows Outlook mail folders to be viewed via web pages. The control should only allow passive operations such as viewing mail or calendar data. In reality, though, it exposes a function that could allow the web page to manipulate Outlook data. In an Outlook 2002 client, this could enable an attacker to delete mail, change calendar information, or take virtually any other action, including running arbitrary code on the user's machine. In contrast, in Outlook 98 and 2000 the attacker could use the control to manipulate the user's folder view, but could not use it to read, change or delete data, or to run code on the user's machine.

Hostile web sites would pose the greatest threat with respect to this vulnerability. If a user could be enticed into visiting a web page controlled by an attacker, script or HTML on the page could invoke the control when the page was opened. The script or HTML could then use the control to take whatever action the attacker desired, within the limits posed by the user's version of Outlook.

It also would be possible for the attacker to send an HTML e-mail to a user, with the intent of invoking the control when the recipient opened the mail. However, the Outlook E-mail Security Update would thwart such an attack. (The Update automatically installs as part of Outlook 2002, and is available for download for Outlook 2000 and 98). The Update causes HTML e-mails to be opened in the Restricted Sites Zone, where ActiveX controls are disabled by default.

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

CVE Link: CVE-2001-0538

Reference: http://www.microsoft.com/technet/security/bulletin/MS01-038.mspx & http://www.sans.org/top20/#W8

- **14450 Unchecked Buffer in Outlook Express S/MIME Parsing Could Enable System Compromise (MS02-058/Q328676)**

To allow for verification of the authenticity of mail messages, Microsoft Outlook Express supports digital signing of messages through S/MIME. A buffer overrun vulnerability lies in the code that generates the warning message when a particular error condition associated with digital signatures occurs.

By creating a digitally signed email and editing it to introduce specific data, then sending it to another user, an attacker could cause either of two effects to occur if the recipient opened or previewed it. In the less serious case, the attacker could cause the mail client to fail. If this happened, the recipient could resume normal operation by restarting the mail client and deleting the offending mail. In the more serious case, the attacker could cause the mail client to run code of their choice on the user's machine. Such code could take any desired action, limited only by the permissions of the recipient on the machine.

This vulnerability could only affect messages that are signed using S/MIME and sent to an Outlook Express user. Users of Microsoft Outlook products are not affected by this vulnerability.

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

CVE Link: CAN-2002-1179

Reference: http://www.microsoft.com/technet/security/bulletin/MS02-058.mspx & http://www.sans.org/top20/#W8

➢ 14451 Symantec AntiVirus Corporate Edition 7.x - 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/

➢ 17899 Linksys Wireless Access Point Identification 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.

It is possible to identify remotely Linksys Wireless access point.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: www.linksys.com

➢ 17902 PHP-Nuke 6.X and 7.X Path Disclosure Vulnerability

Php-Nuke is a popular freeware content management system, written in php by Francisco Burzi. This CMS (Content Management System) is used on many thousands websites, because it's freeware, easy to install and has broad set of features.

Homepage: http://phpnuke.org

It is possible to bypass an internal security check mechanism and determine the installation path.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://securitytracker.com/alerts/2004/Jun/1010355.html

New Vulnerabilities found this Week

❖ Cisco CatOS TCP-ACK Denial Of Service Vulnerability

This vulnerability is documented as Cisco bug IDs CSCec42751, CSCed45576, and CSCed48590. There are techniques available to mitigate the potential effects of this vulnerability in the workaround section of this advisory. Cisco is providing fixed software, and recommends that customers upgrade to it.

http://www.cisco.com/warp/public/707/cisco-sa-20040609-catos.shtml

❖ Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability

A stack-based buffer overflow has been reported in the Apache mod_ssl module.
This issue is exposed in utility code for uuencoding binary data.
This issue would most likely result in a denial of service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures.
http://www.securityfocus.com/bid/10355

❖ 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.
This vulnerability is further exacerbated by the fact that the smbd service runs with root privileges.

http://www.securityfocus.com/bid/7106

❖ Squid Proxy NTLM Authentication Buffer Overflow Vulnerability

Squid Web Proxy Cache is reportedly affected by a buffer overflow vulnerability when processing NTLM authentication credentials. This issue is due to a failure of the application to properly validate buffer boundaries when copying user-supplied input.
This would allow an attacker to modify stack based process memory in order to cause a denial of service condition and execute arbitrary code in the context of the vulnerable web

proxy. This will most likely facilitate unauthorized access to the affected computer.

http://www.securityfocus.com/bid/10500

❖ OpenBSD isakmpd Security Association Deletion Vulnerability

Thomas Walpuski has reported a vulnerability in OpenBSD isakmpd, which can be exploited by malicious people to cause a DoS (Denial of Service) on users' connections.
The vulnerability is caused due to multiple payload handling errors. These make it possible to perform unauthorised deletion of ISAKMP Security Associations (SAs), which identify sessions and are used to describe how communicating entities should use security services.

Successful exploitation allows deletion of arbitrary IPsec tunnels.

http://secunia.com/advisories/11827/

❖ HP-UX ftp Pipe Character Arbitrary Command Execution Vulnerability

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.

http://secunia.com/advisories/11843/

❖ Skype Technologies Skype CallTo URI Handler Buffer Overrun Vulnerability

Skype is reported to be prone to a buffer overrun vulnerability.
The vulnerability is reported to occur due to a lack of bounds checking performed on "callto://" URI data, when a callto URI is followed.
This may result in the corruption of sensitive regions of memory. Ultimately, it is conjectured that this issue may be exploited to execute arbitrary code in the context of a user who follows a malicious URI.

http://www.securityfocus.com/bid/10513

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