netVigilance

ScoutNews Team **1 June 2004**
Issue #22

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review
Top Security News Stories this Week
New Test Cases Tested in SecureScout
New Vulnerabilities this Week

This Week in Review

Financial and insurance segments see increased cyber crime activity.

North Korea admits to using hacking techniques against South Korea to obtain information. At the same time the US Air force has been hacked via South Korea.

The first 64 bit virus has been identified

The Apple OS fix fails to plug the hole.

Enjoy reading

Top Security News Stories this Week

- **Attacks on banks, insurance firms rise.**

Cyberattacks on IT systems of banks and insurance companies are on the rise worldwide, according to a survey released Thursday.
Deloitte Touche Tohmatsu's study showed that nearly 83 percent of respondents said their systems had been compromised in the past year, compared with 39 percent in 2003. Nearly 40 percent of the respondents whose systems were attacked reported financial losses.

http://news.com.com/Attacks+on+banks,+insurance+firms+rise/2100-7349_3-5221629.html?part=rss&tag=feed&subj=news
Denisch C. Sharma

- **North Korea Runs Hackers' Unit**

Military authorities have confirmed that North Korea is collecting information from South Korea through computer hackers.
Song Young-keun, commander of confidential operations, stated on May 27 in his opening speech for the "Conference for National Information Security" at the Korean Air Force Assembly Hall, "Under the direct order of Kim Jong-il, North Korea has been using its elite hacking unit to collect information from our national institutions and research facilities."
http://english.donga.com/srv/service.php3?bicode=060000&biid=2004052816238
Ho-Won Choi

❖ **U.S. Air Force Space Command Hacked**

Several computers of an army unit under the U.S Air Force Space Command (SPACECOM) were hacked by an individual in a third country via a Korean firms' computers in mid-February: Korean police and their U.S counterpart started a joint investigation as.

The U.S. concluded that it was a serious case and hurriedly dispatched its investigators to Korea. The two countries began to find out a closely cooperative investigation system and have shared information to identify the hacker.

http://www.crime-research.org/news/05.25.2004/295

Ludmila Goroshko

❖ **Microsoft To Spend $300 Million on Mega Patch**

Microsoft is issuing a mega patch for Windows XP -- its much-anticipated XP Service Pack 2. The company says the critical update represents a $300 million investment in better security. In addition to being available for download at the Microsoft Web site, XP SP2 will ship with all new PCs.

The security-centric Windows XP update, which had star billing at this week's TechEd conference, will be available as a "critical" download via Microsoft's Windows Update Web site and will ship with all new PCs as part of an agreement with OEMs and computer retailers.

http://www.newsfactor.com/story.xhtml?story_title=Microsoft-To-Spend------Million-on-Mega-Patch&story_id=24271&category=netsecurity

Robin Arnfield

❖ **First 64-bit virus identified**

The virus, called W64.Rugrat.3344, is a "proof-of-concept" virus and is not spreading in the wild, although it is the first known threat to attack 64-bit Windows executables successfully. The threat does not infect 32-bit executables and will not run on 32-bit Windows platforms. It only targets Win64-bit systems.

W64.Rugrat.3344 is a direct-action infector that exits memory after execution. Written in IA64 (Intel Architecture) assembly code, it infects IA64 executable files excluding .dll files. It infects files that are in the same folder as the virus as well as all files within the subfolders.

http://www.globetechnology.com/servlet/story/RTGAM.20040527.gtvirus0527/BNStory/Technology/

Globetechnology

❖ **Mac OS fix fails to plug security hole**

A security hole still threatens Mac OS X users after a patch issued by Apple Computer last week failed to fix the underlying problem, security experts say.

The security issue could allow an attacker to transfer and then run a malicious program on a Mac, if the Mac's user can be enticed to go to a fake Web page on which the program has been placed.

http://www.globetechnology.com/servlet/story/RTGAM.20040526.gtmacmay26/BNStory/Technology/

Robert lemos

New Vulnerabilities Tested in SecureScout

➢ **15486 Cisco IOS SNMP Message Handling Vulnerability**

The Simple Network Management Protocol (SNMP) is a widely deployed protocol that is commonly used to monitor and manage network devices.

There are several types of SNMP messages that are used to request information or configuration changes, respond to requests, enumerate SNMP objects, and send both solicited and unsolicited alerts. These messages use UDP to communicate network information between SNMP agents and managers.

There is vulnerability in Cisco's IOS SNMP service in which attempts to process specific SNMP messages are handled incorrectly. This may potentially cause the device to reload.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml & http://www.us-cert.gov/cas/techalerts/TA04-111B.html & http://www.securityfocus.com/bid/10186/info/

- **15487 Cisco IPSec VPN Services Module Malformed IKE Packet Vulnerability**

A malformed IKE packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router hardware, with the VPNSM installed, to crash and reload.

This vulnerability could be used to conduct a Denial of Service (DoS) attack on the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router hardware platforms that have the VPNSM installed in them. This vulnerability is known to only exist in the modified IKE code which was incorporated in the 12.2SXA, 12.2SXB and 12.2SY Cisco IOS software release trains.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsm.shtml & http://www.securityfocus.com/bid/10083/info/

- **17892 PHP-Nuke 7.3 XSS 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

PHP-Nuke Input Validation Flaw in Union Tap Prevention Feature Permits Cross-Site Scripting Attacks.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://securitytracker.com/alerts/2004/May/1010177.html & http://www.waraxe.us/?modname=sa&id=030

- **17893 PHP-Nuke 6.X and 7.X using PHP 5.X $modpath Arbitrary Commands Execution 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

PHP-Nuke $modpath Include File Flaw May Let Remote Users Execute Arbitrary Commands when using PHP 5.X.

As of PHP 5.0.0 files may be appended via the ftp:// URL wrapper. In prior versions, attempting to append to a file via ftp:// will result in failure.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://securitytracker.com/alerts/2004/May/1010177.html & http://www.waraxe.us/?modname=sa&id=029

- **17895 osCommerce Directory Traversal Vulnerability**

osCommerce is an online shop e-commerce solution under on going development by the open source community. Its feature packed out-of-the-box installation allows store owners to setup, run, and maintain their online stores with minimum effort and with absolutely no costs or license fees involved.

osCommerce combines open source solutions to provide a free and open e-commerce platform, which includes the powerful PHP web scripting language, the stable Apache web server, and the fast MySQL database server.

A directory traversal vulnerability was reported in osCommerce. A remote authenticated administrator can view files on the target system.

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

CVE Link: No CVE Match

Reference: http://securitytracker.com/alerts/2004/May/1010176.html& http://www.oscommerce.com/ & http://www.excluded.org/advisories/advisory13.txt

- **19057 OmniHTTPD Long HTTP Protocol Parameters Vulnerability**

OmniHTTPD is a webserver for Microsoft Windows operating systems. OmniHTTPD supports a number of CGI extensions which provide dynamic content.

Omnihttpd is vulnerable to Cross-site scripting vulnerabilities.

A denial of service vulnerability was reported in Omnicron's OmniHTTPd web server. A remote user can cause the web service to crash.

It is reported that a remote user can send a specially crafted HTTP request with an HTTP version containing 4096 or more characters to cause the web service to crash.

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

CVE Link: CVE-2002-1035

Reference: http://securitytracker.com/alerts/2002/Jul/1004672.html & http://www.securityfocus.com/bid/5136 & http://www.omnicron.ca/

- **17898 phpShop Arbitrary code inclusion Vulnerability**

phpShop is a PHP-based e-commerce application and PHP development framework. phpShop offers the basic features needed to run a successful e-commerce web site and to extend its capabilities for multiple purposes.

If PHP is configured (in php.ini, or otherwise) to have register_globals turned off, then a phpShop installation will initiate a 'fix' to
register all the globals in the HTTP_REQUEST into local variables. One of these variables is the '$base_dir' variable, which is used to declare the base directory of the phpshop installation.

An attacker would only need to create a file called 'phpshop.cfg' on his or her webserver in a directory called 'etc', and craft the base_dir variable to include the code from his webserver,
and the phpShop will include this code into it's page.

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

CVE Link: No CVE Match

Reference: http://securitytracker.com/alerts/2004/May/1010111.html & http://www.phpshop.org/ & http://www.fribble.net/advisories/phpshop_29-04-04.txt

New Vulnerabilities found this Week

- **spamGuard Multiple Buffer Overflow Vulnerabilities**

« heap-based buffer overflows »

Multiple vulnerabilities have been discovered in spamGuard, where some potentially can be remotely exploited by malicious people to compromise a vulnerable system. The vulnerabilities are caused due to boundary errors within several functions. These can be

exploited to cause stack-based and heap-based buffer overflows by passing overly long, specially crafted strings.

Successful exploitation of some of the vulnerabilities may allow execution of arbitrary code.

References :
http://secunia.com/advisories/11747/
http://www.securityfocus.com/bid/10434/info/

❖ **OpenSSL Denial of Service Vulnerabilities**
« denial of service in applications which use OpenSSL »

Three security vulnerabilities have been reported to affect OpenSSL. Each of these remotely exploitable issues may result in a denial of service in applications which use OpenSSL.

The first vulnerability is a NULL pointer assignment that can be triggered by attackers during SSL/TLS handshake exchanges. The CVE candidate name for this vulnerability is CAN-2004-0079. Versions 0.9.6c to 0.9.6k (inclusive) and from 0.9.7a to 0.9.7c (inclusive) are vulnerable.

The second vulnerability is also exploited during the SSL/TLS handshake, though only when Kerberos ciphersuites are in use. The vendor has reported that this vulnerability may not be a threat to many as it is only present when Kerberos ciphersuites are in use, an uncommon configuration.

References :
http://www.securityfocus.com/bid/9899/discussion/

❖ **SquirrelMail "Content-Type:" Header Script Injection Vulnerability**
« script injection attacks »

Román Medina-Heigl Hernández has reported a vulnerability in SquirrelMail, which can be exploited by malicious people to conduct script injection attacks. The vulnerability is caused due to missing input validation of the "Content-Type:" header. This can be exploited via specially crafted emails containing HTML or script code in the "Content-Type:" header to execute the code in a user's browser session in context of a vulnerable site, when the malicious email is viewed.

The vulnerability has been reported in versions 1.4.3-rc1, 1.5.0 and 1.5.1 (cvs). Prior versions may also be affected.

NOTE: A number of other unspecified cross-site scripting vulnerabilities have also been discovered.

References :
http://secunia.com/advisories/11734/

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