netVigilance

ScoutNews Team **30 July 2004**
Issue #31

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

This week we saw an interesting mix of news spanning from a legitimate search engine being used for information gathering for hacking to a business relation where one party accuses the other of hacking.
In addition Sophos is of the opinion that one teenage hacker/script kiddy in Germany is responsible for 70% of all worm activity in first half of 2004.

Enjoy reading

Top Security News Stories this Week

❖ Apple Accuses RealNetworks of Hacking

RealNetworks reaffirms commitment to Harmony software that extends tunes to any player.
Apple has issued a statement accusing RealNetworks of hacker-like tactics for its Harmony technology, which will allow content from Real's music store to be played on Apple's IPod. RealNetworks announced earlier this week that its updated software will let songs downloaded from its own music store be played on a variety of devices. The company quickly shot back to Apple's rebuke, saying it has done nothing wrong, and reaffirming its commitment to developing Harmony.
http://www.pcworld.com/news/article/0,aid,117183,00.asp
Jim Dalrymple

❖ Microsoft releases patch to fix month-old security problem

Microsoft Corp. released a patch Friday to halt the spread of a computer virus that can steal personal information, more than a month after the virus began winding its way through the Internet.
Microsoft had previously released tools to detect the virus and thwart it from infecting computers. But until now, the company did not have a fix available to prevent the pesky virus from spreading.
http://www.siliconvalley.com/mld/siliconvalley/news/editorial/9284368.htm
AP

❖ Google Used as Hacking Tool, Say Experts

Security expert Johnny Long said on Thursday that Google (google.com), the world's most popular search engine, is one of the handiest tools for hackers, according to a report by Cnet. Long, a security researcher for Computer Sciences, said that Google's ability to record the content of Web sites on the Internet can be used to identify those sites that have weak security. For example, a first step to finding vulnerable targets, Long said in the report, is to search for default server page titles, something Google can accomplish with its advanced search options and page caching capabilities. According to the report, the exploitation of Google's in-depth searching capabilities illuminates how software with no malicious motive can be used to help hackers.

http://thewhir.com/marketwatch/goo073004.cfm

Web Host industry review

❖ 70% of viruses written by one man

A report recently published by Sophos has revealed that 70% of all virus activity in the first six months of 2004 can be linked to one German teenager.

Sven Jaschan, 18, is the self-confessed author of the NetSky and Sasser worms which hit Internet users hard in the first six months of the year.

Just two of Jaschan's viruses, the infamous Sasser worm and NetSky, account for almost 50% of all virus activity seen by Sophos up until the end of June. Counting Jaschan's other released variants of the NetSky worm, the total figure accounts for over 70%.

http://itvibe.com/default.aspx?NewsID=2769

Rich Kavanagh

New Vulnerabilities Tested in SecureScout

➢ 13168 MySQL Remote Users Bypass Authentication

A remote user can submit a specially crafted authentication packet to bypass the password authentication mechanims on MySQL. The flaw reportedly resides in the check_scramble_323() function.

A remote user can specify an arbitrary 'passwd_len' value to cause the function to compare a known 'scrambled' password value with a zero-length string. The function reportedly allows a remote user to authenticate successfully with a zero-length string.

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

CVE Links: CAN-2004-0627 & CAN-2004-0628

Reference: http://www.nextgenss.com/advisories/mysql-authbypass.txt & http://www.securityfocus.com/bid/10654

➢ 14257 Buffer Overrun in Messenger Service Could Allow Code Execution (MS03-043/828035) (DCERPC Check)

A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. The vulnerability results because the Messenger Service does not properly validate the length of a message before passing it to the allocated buffer.

An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. The attacker could then take any action on the system, including installing programs, viewing, changing or deleting data, or creating new accounts with full privileges.

The current Test Method can't highlight the presence of the vulnerability on Win NT4 platform.

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

CVE Links: CAN-2003-0717

Reference: http://www.microsoft.com/technet/security/bulletin/MS03-043.mspx

➢ 14267 Vulnerability in Task Scheduler Could Allow Code Execution (MS04-022/841873) (DCERPC Check)

A remote code execution vulnerability exists in the Task Scheduler because of an unchecked buffer.

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. However, user interaction is required to exploit this vulnerability. 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-2004-0212

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-022.mspx

➢ 14461 Mozilla/Firefox shell: protocol security issue

On July 7 a security vulnerability affecting browsers for the Windows operating system was reported to mozilla.org by Keith McCanless, and was subsequently posted to Full Disclosure, a public security mailing list. On the same day, the Mozilla security team confirmed the report of this security issue affecting the Mozilla Application Suite, Firefox, and Thunderbird and discussed and developed the fix at Bugzilla bug 250180. The bug affects only users of Microsoft's Windows operating system. The issue does not affect Linux or Macintosh users.

On July 8th, the Mozilla team released a configuration change which resolves this problem by explicitly disabling the use of the shell: external protocol handler. The fix is available in two forms. The first is a small download which will make this configuration adjustment for the user. The second fix is to install the newest full release of each of these products. Instructions on administering these changes can be found below.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.mozilla.org/security/shell.html & http://www.securityfocus.org/bid/10681/info/

- ### 17711 Apache mod_ssl Stack Overflow Vulnerability

The ssl_util_uuencode_binary() function in 'ssl_util.c' may allow a remote user to supply a specially crafted Subject-DN in a client certificate to trigger the overflow. According to OpenPKG, the overflow resides in the "SSLOptions +FakeBasicAuth" implementation of mod_ssl and can be triggered if the Subject-DN is longer than 6 KB and mod_ssl is configured to trust the certificate's issuing CA.

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

CVE Link: CAN-2004-0488

Reference: http://www.securityfocus.com/bid/10355 & http://www.modssl.org

- ### 17712 Apache mod_ssl Format String Vulnerability

A format string vulnerability was reported in mod_ssl. In certain cases where Apache mod_proxy is also used, a remote user may be able to cause arbitrary code to be executed on the target user's system.

If Apache is used as a proxy and an HTTPS URL such as 'https://foo%s.example.com/' is supplied and a hostname 'foo%s' exists in the 'example.com' zone, the flaw can reportedly be triggered.

The flaw reportedly resides in an error message call in 'ssl_engine_ext.c'.

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

CVE Link: CAN-2004-0700

Reference: http://www.securityfocus.com/bid/10736 & http://www.modssl.org

- ### 17713 Apache mod_ssl memory leak DoS Vulnerability

Memory leak in ssl_engine_io.c for mod_ssl in Apache 2 before 2.0.49 allows remote attackers to cause a denial of service (memory consumption) via plain HTTP requests to the SSL port of an SSL-enabled server.

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

CVE Link: CAN-2004-0113

Reference: http://www.securityfocus.com/bid/9826 & http://www.modssl.org

- ### 17909 SWAT (Samba Web Administration Tool) Buffer Overflows Vulnerability

It has been reported that there is a buffer overflow in the Samba Web Administration Tool

(SWAT) in versions 3.0.2 - 3.0.4. A remote user can supply a specially crafted HTTP Basic Authentication header containing an invalid Base64 character to trigger the overflow and execute arbitrary code on the target system.

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

CVE Link: CAN-2004-0600

Reference: http://www.ibiblio.org/pub/packages/samba/docs/faq/Samba-Server-FAQ.html & http://www.samba.org/ & http://www.securityfocus.com/archive/1/369698/2004-07-21/2004-07-27/0

➢ 17910 PHP-Nuke 7.X Multiple XSS Vulnerabilities

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

- Input passed in the search string in the "Search" module 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.

- Input passed to various parameters in the "Search" module 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.

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

CVE Link: CAN-2004-0737

Reference: http://www.waraxe.us/index.php?modname=sa&id=35 & http://www.waraxe.us/index.php?modname=sa&id=36 & http://phpnuke.org/

➢ 17912 PHP-Nuke 7.X SQL Injection 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

- The "Search" module fails to verify input passed to the "instory" parameter properly before it is used in a SQL query. This can be exploited to manipulate SQL queries.

- The "Search" module fails to verify input passed to the "min" and "categ" parameters properly before it is used in a SQL query. This can be exploited to manipulate SQL queries.

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

CVE Link: CAN-2004-0737

Reference: http://www.waraxe.us/index.php?modname=sa&id=35 & http://phpnuke.org/& http://www.waraxe.us/index.php?modname=sa&id=36

New Vulnerabilities found this Week

- **Mozilla / Mozilla Firefox User Interface Spoofing Vulnerability**

« Spoof the user interface »

A vulnerability has been reported in Mozilla and Mozilla Firefox, allowing malicious websites to spoof the user interface.

The problem is that Mozilla and Mozilla Firefox don't restrict websites from including arbitrary, remote XUL (XML User Interface Language) files. This can be exploited to "hijack" most of the user interface (including tool bars, SSL certificate dialogs, address bar and more), thereby controlling almost anything the user sees.

The Mozilla user interface is built using XUL files.

A PoC (Proof of Concept) exploit for Mozilla Firefox has been published. The PoC spoofs a SSL secured PayPal website.

This has been confirmed using Mozilla 1.7 for Linux, Mozilla Firefox 0.9.1 for Linux, Mozilla 1.7.1 for Windows and Mozilla Firefox 0.9.2 for Windows. Prior versions may also be affected.

NOTE: This issue appears to be the same as Mozilla Bug 244965.

References*:*
http://www.nd.edu/~jsmith30/xul/test/spoof.html
http://bugzilla.mozilla.org/show_bug.cgi?id=244965
http://bugzilla.mozilla.org/show_bug.cgi?id=252198

- **Vulnerability in various Check Point VPN-1 products has been discovered, which can be exploited by malicious people to compromise a system.**
  « Heap overflow »

The vulnerability is caused due to a boundary error in the ASN.1 decoding library during setup of the initial encrypted connection. This can be exploited to cause a heap overflow by establishing a VPN connection and sending a malicious packet containing specially crafted fields.

Successful exploitation does not require any authentication and may allow execution of arbitrary code on a vulnerable system.

References*:*
http://www.checkpoint.com/techsupport/alerts/asn1.html

- **Microsoft Systems Management Server Remote Control Service Vulnerability**

« Denial of Service »

HexView has reported a vulnerability in Microsoft Systems Management Server, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the client SMS Remote Control service when processing specially crafted packets containing the string "RCH0####RCHE" followed by about 130 characters.

Successful exploitation crashes the service.

The vulnerability has been reported in version 2.50.2726.0. Other versions may also be affected.

References*:*
http://secunia.com/advisories/11814/

- **Dropbear SSH Server Digital Signature Standard Unspecified Authentication Vulnerability**

« Authentication vulnerability »

Reportedly Dropbear SSH is affected by an unspecified digital signal standard (DSS) authentication vulnerability; an upgrade is available.

The impact of this issue is currently unknown, although it is speculated that this issue could be used to gain unauthorized access to a computer running the vulnerable application. It should be noted that this is not confirmed. This BID will be updated as more information becomes available.

References:
http://www.securityfocus.com/bid/10803/info/

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