netVigilance

ScoutNews Team **18 July 2004**
Issue #29

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

The computer virus incident report for first half of 2004 in Japan is just one more proof point that you need to be proactive in your security process. Performing in-line on-going vulnerability management using SecureScout has proven to be a good choice.

Hacker Lamo is sentenced and a new online hacker store is closed within weeks of it opening. The good guys are winning some important battles.

Microsoft, AOL and Yahoo among others are determined to make Instant Messaging secure enough for enterprise wide deployment within corporate America.
This just a question of time: As it is the next logical extension of the Internet phenomenon.

Enjoy reading

Top Security News Stories this Week

- **Hacker Lamo Sentenced To Home Detention**

The 'homeless' hacker gets sentenced to six months' home detention and two years' probation by a federal judge.
Adrian Lamo, known as the "homeless" hacker, built a reputation for hacking into the networks of some of America's largest companies and then offering to help, for free, fix the security vulnerabilities that made his incursions possible.
Lamo was indicted for breaking into computer systems at The New York Times. In January, he pleaded guilty to those charges. On Thursday, a federal judge sentenced him to two years probation, with six months to be served in home detention, says Lamo's federal public defender, Sean Hecker.
Lamo will also have to pay $65,000 in restitution, Hecker says
http://www.informationweek.com/story/showArticle.jhtml?articleID=23901163
George V Humle

- **Hacker source code shop closes its doors**

An online shop that was selling the source code for two computer programs has

abruptly suspended its operations, citing a "redesign" of its "business model."
The Source Code Club opened its doors on Monday, using an e-mail posting to an online discussion group to advertise the availability of source code and design documents for two products: the Dragon intrusion detection system (IDS) software from Enterasys Networks Inc. and peer-to-peer (P-to-P) server and client software from Napster LLC, now owned by Roxio Inc. By Thursday, the group's Web page displayed a message saying the Club had ceased operations due to "fears our customers faced."
The group used a Web page with an address in the Ukraine to advertise its wares, saying it was selling "corporate intel(ligence)" to its customers, along with other, unnamed, services, according to a message posted to the Full-Disclosure mailing list by a group or individual using the name "Larry Hobbles."
http://www.infoworld.com/article/04/07/15/HNhackershop_1.html?source=rss&url=http://www.infoworld.com/article/04/07/15/HNhackershop_1.html
Paul Roberts

❖ **MSN, AOL, Yahoo Join on Instant Messaging**
AOL, Microsoft and Yahoo are making an aggressive effort to make instant messaging safe for the enterprise. Though companies increasingly are using the technology, security concerns have caused many to hold back. Microsoft's Office Live Communications Server 2005 is designed to protect the world's largest IM networks.
http://www.newsfactor.com/story.xhtml?story_title=MSN--AOL--Yahoo-Join-on-Instant-Messaging&story_id=25890&category=netsecurity#story-start
Jay Wrolstad

❖ **Be Careful for Dangers Hiding at the Home Page!!**
No, things have not improved compared to last year; in fact looking at the virus incident reports collected by the Information-technology Security Center (ISEC) - Information-technology Promotion Agency (IPA) - Japan -- THINGS GOT WORSE.

1. Computer Virus incident Report for the First Half of 2004

The reported numbers for the first half of 2004 is **21,957** which is about 3 times larger numbers compared with the reported numbers of 7,366 reported in corresponding period of 2003; the yearly reported numbers of 17,425 in 2003 are exceeded sky-high as well.
http://www.ipa.go.jp/security/english/virus/press/200406/E_PR200406.html
Information-technology Promotion Agency, Japan (IPA)

New Vulnerabilities Tested in SecureScout

➢ **14237 ASN.1 Vulnerability Could Allow Code Execution (MS04-007/828028)**
Security vulnerability exists in the Microsoft ASN.1 Library that could allow code execution on an affected system. The vulnerability is caused by an unchecked buffer in the Microsoft ASN.1 Library, which could result in a buffer overflow.

An attacker who successfully exploited this buffer overflow vulnerability could execute code

with system privileges on an affected system. The attacker could then take any action on the system, including installing programs, viewing data, changing data, deleting data, or creating new accounts with full privileges.

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

CVE Links: CAN-2003-0818

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx

- **15360 ASN.1 Vulnerability Could Allow Code Execution (MS04-011/835732)**

A remote code execution vulnerability exists in the Microsoft ASN.1 Library. The vulnerability is caused by a possible "double-free" condition in the Microsoft ASN.1 Library that could lead to memory corruption on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, under the most likely attack scenario this issue is a denial of service vulnerability.

If found vulnerable to this issue and unless you applied specific workarounds, you are also vulnerable to all other vulnerabilities described in the Microsoft Security Bulletin MS04-011.

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

CVE Links: CAN-2003-0533 & CAN-2003-0663 $ CAN-2003-0719 & CAN-2003-0806 & CAN-2003-0906 & CAN-2003-0907 & CAN-2003-0908 & CAN-2003-0909 & CAN-2003-0910 & CAN-2004-0117 & CAN-2004-0118 & CAN-2004-0119 & CAN-2004-0120 & CAN-2004-0123

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

- **17097 Small HTTP Server MS-DOS Device Name DoS Vulnerability**

Versions of Small HTTP server are vulnerable to a denial of service attack.

It is possible to remotely crash a system running Small HTTP server by submitting a URL request for an MS-DOS device name.

A hard reboot of the exploited server is required in order to gain normal functionality.

Test Case Impact: C**rash** Vulnerability Impact: **Crash** Risk: **High**

CVE Link: CVE-2001-0493

Reference: http://www.securityfocus.com/archive/1/179230 &
http://www.securityfocus.com/bid/2649 &
http://wwwwin.wplus.net/pp/mrdoors/srv/index.htm

- **17447 Apache Tomcat Null Character Malformed Request Denial Of Service Vulnerability**

Vulnerability exists in Apache Tomcat 4.0.3 on a Microsoft Windows platform. Reportedly, it is possible for a remote attacker to make requests consisting of a large number of null characters to Tomcat that will cause the web service to stop responding.

By making numerous malformed requests, the attacker is able to exhaust all available threads for Tomcat leading to the denial of service condition

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

CVE Link: CVE-2002-0935

Reference: http://online.securityfocus.com/archive/1/277940 & http://www.securityfocus.com/bid/5067 & http://jakarta.apache.org/tomcat/index.html

- 17588 Apache Tomcat on HP Directory Disclosure Vulnerability

Apache Tomcat is reported to be prone to a vulnerability which may enable remote attackers to disclose the contents of directories.

This issue is reported to affect Apache Tomcat 3.2.x on HP-UX 11.04 (VVOS) systems.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.securityfocus.com/advisories/4511 & http://www.securityfocus.com/bid/5838 & http://jakarta.apache.org/tomcat

- **17601 Apache Tomcat DefaultServlet File Disclosure Vulnerability**

The servlet "org.apache.catalina.servlets.DefaultServlet" is included with Apache Tomcat by default. It is possible to use this servlet to view contents of files within the webroot. This includes JSP source code which may contain sensitive data such as database usernames and passwords.

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

CVE Link: CAN-2002-1394 & CAN-2002-1148

Reference: http://www.securityfocus.com/bid/5786 & http://jakarta.apache.org/tomcat

- **17679 ASN.1 Vulnerability Could Allow Code Execution (MS04-007/828028)**

A security vulnerability exists in the Microsoft ASN.1 Library that could allow code execution on an affected system. The vulnerability is caused by an unchecked buffer in the Microsoft ASN.1 Library, which could result in a buffer overflow.

An attacker who successfully exploited this buffer overflow vulnerability could execute code with system privileges on an affected system. The attacker could then take any action on the system, including installing programs, viewing data, changing data, deleting data, or creating new accounts with full privileges.

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

CVE Link: CAN-2003-0818

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx

- **17822 Instant servers Mini portal 1.1.5 Buffer Overflow Vulnerability**

Instantservers product miniportal 1.1.5 is a shareware ftp/webserver. It has been discovered that there is a buffer overflow in the ftp server which when exploited causes the server to crash creating a denial of service.

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

CVE Link: CAN-2002-0260

Reference: http://marc.theaimsgroup.com/?l=bugtraq&m=101329397901071&w=2 & http://www.instantservers.com/releases.html

- **17906 Apache httpd Header Line Memory Allocation Vulnerability**

The remote Apache server, according to its version number, might allow a denial of service vulnerability.

This vulnearbility was reported in the Apache web server in the folding of header lines. A remote user can cause the application to consume arbitrary amounts of memory.

It has been reported that a remote user can send header lines that begin with a tab or space character to cause ap_get_mime_headers_core() in 'server/protocol.c' to allocate memory for the header line. A remote user can reportedly send a large number of specially crafted header lines to cause Apache to consume all available memory on the target system and crash.

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

CVE Link: CAN-2004-0493

Reference: http://www.guninski.com/httpd1.html & http://httpd.apache.org

- **17908 I-Mall Shell Commands Injection Vulnerability**

I-mall.cgi is reported prone to a remote arbitrary command execution vulnerability. This issue presents itself due to insufficient sanitization of user-supplied data and may allow a remote attacker to pass arbitrary shell commands to the vulnerable script.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.zone-h.org/en/advisories/read/id=4904/ & http://securitytracker.com/alerts/2004/Jun/1010609.html

New Vulnerabilities found this Week

- **ISC DHCPD VSPRINTF Buffer Overflow Vulnerability**

“remotely exploitable buffer overflow”

ISC DHCPD is reported likely vulnerable to remotely exploitable buffer overflow vulnerabilities on systems which lack a vsnprintf() library function.

On systems which lack the vsnprintf() library call, ISC DHCPD defines vsnprintf as:
#define vsnprintf(buf, size, fmt, list) vsprintf (buf, fmt, list)

This definition discards the size argument to the function, potentially allowing any occurrence of vsnprintf() to be exploitable, by overflowing whatever intended buffer is passed to the library call.

Other locations in DHCPD utilizing this function may be exploitable. Successfully exploiting this issue may lead to a denial of service condition, or remote code execution in the context of the DHCPD server.

This issue is reported to affect ISC DHCPD versions 3.0.1rc12 and 3.0.1rc13.

References : http://www.securityfocus.com/archive/1/367286

- **ISC DHCPD Hostname Options Logging Buffer Overflow Vulnerability**

"remotely exploitable buffer overflow"

ISC DHCPD is prone to a remotely exploitable buffer overflow vulnerability. This issue exists in routines responsible for logging hostname options provided by DHCP clients. Successful exploitation could result in execution of arbitrary code in the context of the DHCPD server.

This issue is reported to affect ISC DHCPD versions 3.0.1rc12 and 3.0.1rc13. The vulnerable code exists in previous versions of ISC DHCPD 3, but is only believed to be exploitable in these two releases.

References : http://www.securityfocus.com/archive/1/367286

- **NullSoft Winamp Long File Name Denial of Service Vulnerability**

"denial of service vulnerability"

It has been reported that Winamp may be prone to a denial of service vulnerability when processing files with a name exceeding 246 characters. Immediate consequences of this issue may result in the application crashing. Although unconfirmed, due to the nature of this vulnerability an attack could result in a buffer overflow condition and may lead to arbitrary code execution. Any code execution would occur in the context of the user running the application.

Winamp 5.02 was identified as the vulnerable version, however, it is possible that other versions are affected as well.

Conflicting reports have surfaced regarding this issue. It is possible that this issue may not be valid. This BID will be updated or retired as more information becomes available.

References : http://www.securityfocus.com/bid/9920/discussion/

- **PHP "strip_tags()" Function and memory_limit Vulnerabilities**

"cross-site scripting attacks, execute arbitrary code"

Stefan Esser has reported two vulnerabilities in PHP, which can be exploited by malicious people to bypass certain security functionality or compromise a vulnerable system.

1) The "strip_tags()" function fails to strip obfuscated HTML tags (e.g. tags with "\0"). This can be exploited to conduct cross-site scripting attacks against sites, which only rely on the "strip_tags()" functionality to prevent such attacks.

NOTE: An HTML tag such as "<script>" with an embedded binary character like "\0" is not a valid HTML entity. However, certain browsers such as Internet Explorer and Safari strip such illegal characters and render it. This is not a vulnerability in those browser, but unfortunate and unnecessary functionality.

2) Various errors within PHP's memory_limit request termination (e.g. when allocating Zend HashTables before proper initialisation) can be exploited to execute arbitrary code by corrupting the heap (e.g. supplying arbitrary HashTable destructor pointers).

Successful exploitation requires that a resource limit has been set via the "memory_limit" configuration directive.

The vulnerabilities have been reported in version 4.3.7 and prior and version 5.0.0RC3 and prior.
References : http://security.e-matters.de/advisories/112004.html

- **mod_ssl Unspecified "mod_proxy" Hook Functions Format String Vulnerability**

A vulnerability has been reported in mod_ssl, which currently has an unknown impact but may allow malicious people to compromise a vulnerable system.

The vulnerability is reportedly caused due to a "ssl_log()" related format string error within the "mod_proxy" hook functions.
References : http://secunia.com/advisories/12077/

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