**ScoutNews Team** **3 July 2004**
**Issue #27**

Weekly ScoutNews by netVigilance

**Table of Contents**



# This Week in Review

You may have been wondering why the number of testcases in SecureScout testing for something as benign as addware/spyware increased during the past 4-6 months.

**Now you know!**

Last weeks occurrence of a browser based worm that used adware/spyware type methods to infect workstations and steal password and bank account information is the first in a new wave of blended attacks.

Luckily SecureScout has been adding testcases for the most dangerous Spy-and Addware incidents so you have received the warnings to remedy these vulnerabilities in your scanning reports for some time.

This is not to say that SecureScout will become an addware/spyware cleaner, however SecureScout focuses on the high impact variants that could leave your network wide open for compromising and malicious attacks.

Enjoy reading

# Top Security News Stories this Week

- **Microsoft Issues Security Update For Trojan**

Microsoft (Quote, Chart) is urging customers to immediately install a security update for Windows XP, Windows Server 2003 and Windows 2000 operating systems in order to thwart the impact of the Download.Ject Trojan.
The software giant said the configuration changes would "improve system resiliency" against the Download.Ject attack and protect customers against the immediate reported threats. The changes to the operating systems are meant to plug holes that could help spread malicious files by infected computers.
The update comes in the wake of a recent sophisticated attack against Microsoft's IIS 5.0 servers, which ended when law enforcement took the Web site associated with the attack offline.

Download.Ject, also known as Scob, is a Trojan downloader that started spreading a week ago after attackers planted a file with JavaScript to infected Web sites running Microsoft IIS 5.0 servers.
http://www.internetnews.com/security/article.php/3376951
Susan Kuchinskas

❖ **Russian Hacker Team Behind Last Week's Web Attack**

The Trojan downloaded to PCs from compromised IIS servers was almost certainly the work of HangUP, a security firm said Thursday, more proof that the infamous Russian hacker group was behind last week's Web attack.
F-Secure's analysis of the Padador/Qukart code discovered a “copyright” message in the first seven variants. According to the Finnish security firm, the Trojan contain the phrase “Padonok coded by HangUP Team.”
http://www.techweb.com/wire/story/TWB20040702S0002
TechWeb News

❖ **New Lovegate worm spreading**

It's infecting computers worldwide, including those at some Fortune 500 firms
A new version of the Lovegate worm has begun infecting computers worldwide, including those belonging to several Fortune 500 companies, according to a statement from antivirus firm McAfee Inc.
Like its predecessors, Lovegate.ad@MM is a mass-mailing worm that spreads through e-mail and network file sharing and by exploiting a previously disclosed vulnerability in the remote procedure call interface in multiple Windows versions. Last year's widespread Blaster worm took advantage of the same flaw.
http://www.computerworld.com/securitytopics/security/virus/story/0,10801,94290,00.html
Jaikumar Vijayan

❖ **Crackers Unleash Spyware Tactics on IE Holes**

The rash of recent attacks exploiting vulnerabilities in Microsoft Corp.'s Internet Explorer browser is evidence that crackers are adopting tactics favored by spyware purveyors and could just be the beginning of a wave of highly targeted, well-engineered attacks, security experts say.
http://www.eweek.com/article2/0,1759,1619842,00.asp?kc=EWRSS03119TX1K0000594
Dennis Fisher

# New Vulnerabilities Tested in SecureScout

➢ **17077 John Roy Pi3Web viewenv CGI Vulnerability**

John Roy Pi3Web is a standard web server which includes CGI and ISAPI support. Pi3Web uses multithreading to handle system requests. Pi3Web is available for Windows, Linux and Solaris.
It has been reported that Pi3Web viewenv if not deleted, discloses all environment variables. This information may be aid in further attacks against the host running the vulnerable software.
This issue was reported for the Microsoft Windows version of the software. Versions that run

on other platforms may also be affected.

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

**CVE Links:** GENERIC-MAP-NOMATCH

**Reference:** http://online.securityfocus.com/archive/1/260734 & http://www.securityfocus.com/bid/4261 & http://pi3web.sourceforge.net/pi3web/

### ➢ 17080 Apache Tomcat 3.0 & 3.2.1 Directory Traversal Vulnerability

Apache Tomcat contains a traversal directory condition, that allows to gain access to files outside of the root directory.

Appending a requested URL by '/../' sequences, allows an attacker to obtain read access to directories and files outside of the normal structure. In this way, an attacker can disclose sensitive information such as user data and/or system data that can be used for further attacks.

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

**CVE Links:** GENERIC-MAP-NOMATCH

**Reference:** http://www.securityfocus.com/archive/1/172168 & http://www.securityfocus.com/bid/2518 & http://www.securityfocus.com/archive/1/172611 & http://www.securityfocus.com/archive/1/172612

### ➢ 17297 John Roy Pi3Web Long Request Buffer Overflow Vulnerability

Pi3Web is a free, multithreaded, highly configurable and extensible HTTP server and development environment for cross platform internet server development and deployment. Pi3Web can be ran under Windows, Linux and Solaris.
A buffer overflow vulnerability exists in John Roy Pi3Web web server. An attacker can cause the server to stop responding and possibly execute code.
This is due to the CGI parameter's handling of unusually crafted requests.

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

**CVE Link:** CAN-2002-0142

**Reference:** http://www.securityoffice.net/articles/pi3web/ & http://www.securityfocus.com/bid/3866 & http://pi3web.sourceforge.net/pi3web/

### ➢ 17326 Lotus Domino MS-DOS Device Name DOS Vulnerability

Lotus Domino is an application server developed by IBM.
Some versions up to 5.0.9 are vulnerable to denial of service : when 400 MS-DOS devicename ( AUX, CON, COM ) requests are sent to the server, the server stops processing more requests.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://www.securityfocus.com/archive/1/253830 & http://www.securityfocus.com/bid/4019 & http://www.lotus.com/home.nsf/welcome/domino

### ➢ 17372 John Roy Pi3Web File Disclosure Vulnerability

John Roy Pi3Web is a standard web server which includes CGI and ISAPI support. Pi3Web uses multithreading to handle system requests. Pi3Web is available for Windows, Linux and Solaris.
Pi3Web is prone to an issue which may cause arbitrary web-readable files to be disclosed to remote attackers. A remote attacker is able to gain a listing of files by submitting a request containing a wildcard (*), followed by the file extension of the type of file they wish to disclose. For example:
http://pi3web-host.com/*.extension
This issue was reported for the Microsoft Windows version of the software. Versions that run on other platforms may also be affected. It should also be noted that webservers on the Microsoft Windows platform normally run with SYSTEM privileges.

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

**CVE Link:** CAN-2002-0433

**Reference:** http://online.securityfocus.com/archive/1/260734 & http://www.securityfocus.com/bid/4262 & http://pi3web.sourceforge.net/pi3web/

### ➢ 17375 PHP ImgList Directory Traversal Vulnerability

PHP ImgList allows a user to generate a web gallery of image files.
A vulnerability exists in PHP ImgList which allows a remote user to traverse the directories of a target host. This may lead to the disclosure of file and directory contents. Arbitrary directories can be accessed through the use of double dot '../' techniques

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

**CVE Link:** CVE-2002-0441

**Reference:** http://online.securityfocus.com/archive/1/261221 & http://online.securityfocus.com/archive/1/261225 & http://www.liquidpulse.net/s.lp?id=17

### ➢ 17460 MyWebServer Buffer Overflow Vulnerability

MyWebServer is a free personal peer-to-peer web, file and application server. A buffer overflow condition is contained in versions 1.02 and previous of MyWebServer.
Exploitation of this vulnerability allows remote execution of arbitrary code with daemon privileges.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://www.foundstone.com/knowledge/randd-advisories-display.html?id=330 & http://www.mywebserver.org

- 17516 SquirrelMail SquirrelSpell Remote Shell Command Execution Vulnerability

This testcase checks that shell interpreters (as, sash,sh, csh, and so on) are or aren't installed in the cgi-bin directory.
This is a common mistake made by administrators in their configuration since even some webserver installation guides advised CGI script interpreters should be located in the cgi-bin directory.
This flaw allows a remote attacker to perform arbitrary commands by passing parameters to the interpreters.

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

**CVE Link:** CAN-1999-0509

**Reference:** http://www.cert.org/advisories/CA-1996-11.html & http://www.sans.org/top20/#U3 & http://www.sans.org/top20/#W1

- **17549 CGI Script Interpreters Inside cgi-bin Directory Vulnerability**

Squirrelmail is a PHP based mail system designed for integration into an existing mail server system to allow a remote user to access his mail via the web.

Squirrelmail comes with many in-built modules which allow for various functionality. One of these modules "squirrelspell" is a built in spell checker system integrated into squirrelmail.

There exists in the squirrelspell module a vulnerability which allows a remote user to execute any piece of code or command that they chose.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://online.securityfocus.com/bid/3952 & http://www.squirrelmail.org & http://online.securityfocus.com/archive/1/252156

- **17886 Apache Connection Denial of Service Vulnerability**

Vulnerability has been reported in Apache, which can be exploited by malicious people to cause a Denial of Service.

The problem is that when using multiple listening sockets, a short lived connection on a rarely used socket causes the child process to hold the accept mutex, thereby preventing new connections from being served until another connection uses the socket.

This has been reported to affect Apache 1.3.29/2.0.48 and prior on some versions of AIX, Solaris, and Tru64.

Linux, FreeBSD, and Windows are not affected.

If HeavyScan option is used, Operating System Version is not taken into account, so this TestCase may generate false positive when testing OS not in AIX, Solaris and Tru64 Family.

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

**CVE Link:** CAN-2004-0174

**Reference:** http://www.apache.org/dist/httpd/Announcement2.html & http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0174

# New Vulnerabilities found this Week

- **Multiple Browsers Frame Injection Vulnerability**

« spoof the content of websites »
A 6 year old vulnerability has been discovered in multiple browsers, allowing malicious people to spoof the content of websites.

The problem is that the browsers don't check if a target frame belongs to a website containing a malicious link, which therefore doesn't prevent one browser window from loading content in a named frame in another window.

Successful exploitation allows a malicious website to load arbitrary content in an arbitrary frame in another browser window owned by e.g. a trusted site.

Secunia has constructed a test, which can be used to check if your browser is affected by this issue:
http://secunia.com/multiple_browsers_frame_injection_vulnerability_test/

The vulnerability has been confirmed in the following browsers:
* Opera 7.51 for Windows
* Opera 7.50 for Linux
* Mozilla 1.6 for Windows
* Mozilla 1.6 for Linux
* Mozilla Firebird 0.7 for Linux
* Mozilla Firefox 0.8 for Windows
* Netscape 7.1 for Windows
* Internet Explorer for Mac 5.2.3
* Safari 1.2.2
* Konqueror 3.1-15redhat

Other versions may also be affected.

The vulnerability also affects Internet Explorer:
SA11966

References : http://secunia.com/advisories/11966/

- **Apache Mod_Proxy Remote Negative Content-Length Buffer Overflow Vulnerability**

« remote buffer overflow »
A remote buffer overflow vulnerability exists in Apache mod_proxy.

The source of this issue is that a negative user-specified length value may be used in a memory copy operation, allowing for corruption of memory. This may triggered if a remote server returns a negative Content-Length: HTTP header field to be passed through the proxy.

Exploitation will likely result in a denial of service, though there is an unconfirmed potential for execution of arbitrary code on some platforms (such as BSD implementations). Versions that have the optional AP_ENABLE_EXCEPTION_HOOK define enabled may also be exploitable on some platforms.

This issue affects Apache servers 1.3.26 through 1.3.31 that have mod_proxy enabled and configured. Apache 2.0.x releases are not affected by this issue.

References : http://www.securityfocus.com/bid/10508/discussion/

- **Open WebMail Vacation.PL Remote Command Execution Variant Vulnerability**

« execute arbitrary commands »
A vulnerability is reported in Open WebMail that allows a remote attacker to execute arbitrary commands on a vulnerable host.

Exploitation of the vulnerability could allow a non-privileged user to remotely execute arbitrary commands in the context of the web server that is hosting the vulnerable application.

This vulnerability is reported to affect all versions of Open WebMail released before 29/06/2004.

References : http://www.securityfocus.com/bid/10637/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