netVigilance

ScoutNews Team **10 September 2004**
Issue #37

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

There is lots of news out there this week.
Most of the “news” is a rehash of old topics like the increased complexity and danger of blended attacks, VOIP Spam on its way and viruses for cell phones.
We have chosen to include three stories on the legal front.

Enjoy reading

Top Security News Stories this Week

- **MyDoom worm creators ask for job in anti-virus industry, Sophos reports**
  The creators of the latest versions of the MyDoom email worm have embedded a secret message inside their code, asking for a job in the anti-virus industry, researchers at Sophos have discovered.

http://www.sophos.com/virusinfo/articles/mydoomuvw.html
Sophos

- **Developer considers McAfee suit after 'Trojan' error**
  Brisbane software developer Mark Griffiths is considering suing McAfee after the antivirus company wrongly identified his Internet setup program as a Trojan in a recent virus definition update.

http://news.zdnet.co.uk/software/developer/0,39020387,39166163,00.htm
Kristyn Maslog-Levis

- **Teenager charged over Sasser worm**
  The German teenager who allegedly wrote the Sasser and Netsky computer worms has been charged.
  Sven Jaschan, now 18, was arrested in May this year at his parents' home in Waffensen, North Germany.
  He has now been charged with computer sabotage, which carries a maximum five-year jail term.

http://www.vnunet.com/news/1157975
Dinah Greek

New Vulnerabilities Tested in SecureScout

- **15814 Cisco SSH Malformed Packet Vulnerabilities (CSCdz60229/CSCdy87221/CSCdu75477)**
  Certain Cisco products containing support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS® is disabled by default.

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

CVE Links: CAN-2002-1357 & CAN-2002-1358 & CAN-2002-1359 & CAN-2002-1360

Reference: http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

- **15819 Cisco Scanning for SSH Can Cause a Crash (CSCdw33027)**
  While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities (http://www.cisco.com/warp/public/707/SSH-multiple-pub.html) Cisco inadvertently introduced an instability in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device.

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

CVE Links: CVE-2002-1024

Reference: http://www.cisco.com/warp/public/707/SSH-scanning.shtml

- **15843 Cisco Multiple Product Vulnerabilities Found by PROTOS SIP Test Suite (CSCdz39284/CSCdz41124)**
  Multiple Cisco products contain vulnerabilities in the processing of Session Initiation Protocol (SIP) INVITE messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for SIP and can be repeatedly exploited to produce a denial of service.

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-20030221-protos.shtml

- **15871 Cisco IOS Accepts ICMP Redirects in Non-default Configuration Settings (CSCdx92043)**
  By sending bogus ICMP redirect packets a malicious user can either disrupt or intercept communication from a router.

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

CVE Link: CAN-2002-1222

Reference: http://www.securityfocus.com/archive/1/311336

- **15909 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdx54675)**
  The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

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

CVE Link: CAN-2002-1102

Reference: http://www.cisco.com/warp/public/707/vpn3k-multiple-vuln-pub.shtml

- **1**9288 **Hijack NetSpry**
  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/n/netspry.asp

- **19289 Hijack NetworkEssentials.SCBar**
  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/n/networkessentials_scbar.asp

- **19290 Hijack NowBox**
  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/n/nowbox.asp

- **19292 Hijack PeopleOnPage.AproposMedia**
  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/p/peopleonpage_aproposmedia.asp

- **19294 Hijack PopUpDefence**
  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/p/popupdefence.asp

- **19295 Hijack PopUp Network**
  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/p/popup_network.asp

New Vulnerabilities found this Week

- **Kazaa Altnet Download Manager Buffer Overflow Vulnerability**

CelebrityHacker has reported a vulnerability in the Altnet Download Manager included in Kazaa, which can be exploited by malicious people to compromise a user's system.
The vulnerability has been confirmed in Altnet Download Manager 4.0.0.4 included in Kazaa

2.7.1. Other versions may also be affected.

References: http://secunia.com/advisories/12446/

❖ **Trillian MSN Module Buffer Overflow Vulnerability**

Komrade has reported a vulnerability in Trillian, which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a boundary error within the MSN module. This can be exploited to cause a buffer overflow by passing an overly long string (about 4096 bytes) from a MSN messenger server.
Successful exploitation requires that a malicious person either intercepts and manipulates traffic sent from a MSN messenger server to the user or get the user's Trillian to connect to a malicious MSN messenger server.
The vulnerability has been reported in version 0.74i. Other versions may also be affected.

References: http://unsecure.altervista.org/security/trillian.htm

❖ **Usermin Shell Command Injection and Insecure Installation Vulnerabilities**

"Execution of arbitrary commands"
Two vulnerabilities have been reported in Usermin, where the most critical can be exploited by malicious people to compromise a vulnerable system.
1) An input validation error within the web mail functionality can be exploited to inject arbitrary shell commands, which will be executed when a user views a specially crafted HTML mail.
Successful exploitation allows execution of arbitrary commands with the privileges of the Usermin user.
This vulnerability has been reported in versions 1.070 and 1.080.
2) Malicious, local users can exploit an unspecified error within the installation routine by creating the "/tmp/.webmin" directory before the installation routine does so.
This vulnerability has an unknown impact.

References: http://www.webmin.com/uchanges.html

❖ **ImageMagick BMP Image Decoding Buffer Overflow Vulnerability**

A vulnerability has been reported in ImageMagick, which potentially can be exploited by malicious people to compromise a user's system.

References: http://studio.imagemagick.org/pi...velopers/2004-August/002011.html

❖ **mpg123 Mpeg Layer-2 Audio Decoder Buffer Overflow Vulnerability**

"Buffer overflow, allow execution of arbitrary code"
Davide Del Vecchio has reported a vulnerability in mpg123, which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to an error within the "do_layer2()" function in the Mpeg layer-2 audio decoder. This can be exploited to cause a buffer overflow via a specially crafted mpeg audio file.
Successful exploitation may allow execution of arbitrary code with the privileges of the user executing mpg123.
The vulnerability has been reported in version 0.59r. Other versions may also be affected.

References: http://www.alighieri.org/advisories/advisory-mpg123.txt

❖ **imlib/imlib2 BMP Image Decoding Buffer Overflow Vulnerability**

"Execution of arbitrary code"

Marcus Meissner has reported a vulnerability in imlib and imlib2, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the decoding of runlength-encoded BMP images. This can be exploited to cause a buffer overflow by tricking a user into viewing a specially crafted BMP image.

Successful exploitation may allow execution of arbitrary code.

References: http://bugzilla.gnome.org/show_bug.cgi?id=151034

❖ **CuteNews Inclusion of Arbitrary Files and Cross-Site Scripting**

"Include arbitrary files from external and local resources, execute arbitrary HTML and script code"

Two vulnerabilities have been reported in CuteNews, allowing malicious people to compromise a vulnerable system or conduct cross-site scripting attacks.

1) The "cutepath" parameter in "show_archives.php" and "show_news.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources.

2) Input passed to the "mod" parameter in "index.php" 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.

The vulnerabilities have been reported in version 1.3.6. Prior versions may also be affected.

References:
http://www.7a69ezine.org/node/view/130
http://www.hackgen.org/advisories/hackgen-2004-001.txt

❖ **gnubiff POP3 Buffer Overflow and Denial of Service Vulnerabilities**

"Denial of Service"

Two vulnerabilities have been reported in gnubiff, which potentially can be exploited to cause a DoS (Denial of Service) or compromise a vulnerable system.

1) An unspecified boundary error exists within the POP3 functionality. This can be exploited to cause a buffer overflow and may potentially allow execution of arbitrary code.

2) An error within the POP3 functionality when processing UIDL lists can be exploited to disrupt the functionality and eventually crash the process via an infinite UIDL list.

References: http://sourceforge.net/project/showfiles.php?group_id=94176

❖ **Squid NTLM Authentication Denial of Service Vulnerability**

"Denial of Service"

Marco Ortisi has reported a vulnerability in Squid, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to insufficient validation of negative values in the function "ntlm_fetch_string()" in "lib/ntlmauth.c". This can be exploited by sending a specially crafted NTLMSSP packet, which can cause the NTLM helpers provided by Squid to crash.

Successful exploitation requires that NTLM authentication is enabled.
The vulnerability has been reported in version 2.5.

References:
http://www.squid-cache.org/bugs/show_bug.cgi?id=1045
http://www1.uk.squid-cache.org/s...id-2.5.STABLE6-ntlm_fetch_string

❖ **vpopmail SQL Injection Vulnerabilities**

"SQL injection attacks"
Some vulnerabilities have been reported in vpopmail, which can be exploited by malicious people to conduct SQL injection attacks.
The vulnerabilities are caused due to some unspecified input validation errors, which allows manipulation of SQL queries used for POP/IMAP login, SMTP AUTH, and QmailAdmin login by injecting arbitrary SQL code.
Successful exploitation requires that a SQL backend is used.
The vulnerabilities reportedly affect version 5.4.5 and prior.
NOTE: A potential boundary error has also been reported, which possibly could be exploited by malicious, adminstrative users to cause a buffer overflow when adding new users.

References:
http://sourceforge.net/forum/forum.php?forum_id=400873
http://www.kupchino.org.ru/unl0ck/advisories/vpopmail.txt

❖ **Sun Solaris in.named Remote Denial of Service Vulnerability**

"Remotely exploitable denial of service"
Sun has reported that a remotely exploitable denial of service affects the Solaris 8 version of in.named, the primary DNS daemon. According to the report, a remote attacker can crash a running in.named process by sending it dynamic updates. Sun has stated that the remote attacker must be "privileged".
Sun had made patches available. It is not known if this vulnerability is present in the ISC BIND source tree. If this were so, many other systems would be affected.

References: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57614-1

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