netVigilance

ScoutNews Team

6 August 2004
Issue #32

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

This week we saw more variants of well known worms, Mozilla using a bounty to try to get ahead on vulnerabilities discovered, Singapore conducting an official hacking competition and more Blog spamming happening.
These are all events in the ongoing churn in our online security evolution.

The FCC has ruled that internet based technologies replacing common telephony shall be governed by the same laws as traditional applications. At the same time we are starting to see source code being stolen from outsource locations in India.
These events raise the question: Can we expect the same legal environment as we are used to while achieving a five fold reduction in cost of development?

Enjoy reading

Top Security News Stories this Week

❖ Latest MyDoom hunts victims via Yahoo!

Another new version of the MyDoom worm is spreading, and like last week's variant it uses Yahoo! as part of its infection routine.
MyDoom-Q is similar to earlier MyDoom variants. It normally spreads via email, with a spoofed sending address and a variety of different subject lines. The body of an infected email contains random sentences, some of which refer to the attached Zip file that contains viral code. Once opened, this payload file copies itself to the Windows system directory as "winlibs.exe." The executable contains a list of dozens of common first and surnames that it puts through Yahoo's 'People Search' function in an attempt to find more email addresses to target for infection. It also scours files on the infected user's hard drive for future potential victim.
http://www.theregister.co.uk/2004/08/04/mydoom_targets_yahoo/
John Leyden

❖ Mozilla Foundation Announces Security Bug Bounty Program

Program harnesses power of the open source community to identify security vulnerabilities before they are exploited.
The Mozilla Foundation today announced the Mozilla Security Bug Bounty Program, an initiative that rewards users who identify and report security vulnerabilities in the

open source project's software. Under the new program, users reporting critical security bugs - as judged by the Mozilla Foundation staff - will collect a $500 cash prize. The new initiative was launched with funding from leading Linux software developer Linspire, Inc., and renowned Internet entrepreneur Mark Shuttleworth.
http://www.net-security.org/press.php?id=2329
HNS

❖ Singapore to hold computer hacking contest

Singapore is organizing a contest to find the tech-savvy city-state's best computer hacker.
Six pairs will compete in the Aug. 20 BlackOPS: HackAttack Challenge 2004, organized by the government-funded National Infocomm Competency Center, its marketing manager Yvonne Choo said.
They will "penetrate, exploit, gain access and obtain privileged information from the other teams' servers, for the purpose of corporate espionage," the centre said on its Web site Tuesday.
http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1091624260546_67/?hub=SciTech
AP

❖ Porno blog spam turns nasty

Blog spamming is turning nasty. First spotted approximately a year ago, blog spam involves the automated posting of Web address onto weblogs or online discussion boards.
Spam comments deposited using the technique include a link to a spamvertised website. The idea is not so much to get visitors to a spammed location to visit the promoted site but to increase its page rankings in Google. This, in turn, increases the prominence of the site in certain searches and therefore increases the likelihood that more visitors will visit a site. That's the theory anyway.
http://www.theregister.co.uk/2004/08/04/porno_blog_spam/
John Leyden

❖ FCC rules on fiber-optic networks, wiretaps

The Federal Communications Commission gives the Baby Bells a boost and issues a surprise ruling on TiVo. Also: Eavesdropping rules apply to Net phones.
http://news.com.com/FCC+rules+on+spam%2C+wiretaps/2009-1030_3-5296770.html

❖ Source code stolen from U.S. software company in India

Jolly Technologies, a division of U.S. Company Jolly Inc., reported Wednesday that an insider stole portions of the source code and confidential design documents relating to one of its key products, at its research and development center in Mumbai, India. The company has as a result halted all development activities at the center.
Jolly Technologies is a vendor of labeling and card software for the printing industry. It set up its research and development facility in Mumbai less than three months ago, according to a press release from the parent company.
The company said in the release that according to a report obtained from its branch in India, a recently hired software engineer used her Yahoo Inc. e-mail account, which now allows 100MB of free storage space, to upload and ship the copied files out of the research facility. After detecting the theft, the company is trying to prevent the

employee from further distributing the source code and other confidential information, the company said.
http://www.infoworld.com/article/04/08/05/HNcodestolen_1.html
John Ribeiro

New Vulnerabilities Tested in SecureScout

➢ 19057 Hijack Lycos Sidesearch

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.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/l/lycos_sidesearch.asp

➢ 19058 Hijack MadFinder

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.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/m/madfinder.asp

➢ 19059 Hijack MediaUpdate

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.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/m/mediaupdate.asp

➢ 19060 Hijack MemoryMeter

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.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/m/memorymeter.asp

- **19061 Hijack MSInfoSys**

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.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/m/msinfosys.asp

- **19062 Hijack MyPageFinder**

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.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: L**ow**

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/m/mypagefinder.asp

- **19063 Hijack NavExcel**

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.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/n/navexcel.asp

- **19064 Hijack NCase**

nCase.Inst is an ActiveX drive-by installer that will load nCase.msbb. This installer may be built into ads at some web sites. nCase is also bundled with many applications, including file sharing programs, FavoriteMan, and BookedSpace.

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.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/n/ncase.asp

- **19065 Hijack NetSource101**

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.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/n/netsource101.asp

New Vulnerabilities found this Week

- **libpng Multiple Vulnerabilities**

“Denial of Service”

Chris Evans has discovered multiple vulnerabilities in libpng, which can be exploited by malicious people to compromise a vulnerable system or cause a DoS (Denial of Service).

The vulnerabilities are caused due to NULL pointer dereference errors and boundary errors within various functions when processing PNG files. Some of these can be exploited to cause stack-based buffer overflows via specially crafted PNG files.

The vulnerabilities can e.g. be exploited by tricking a user into visiting a malicious website or view a malicious email with an affected application linked to libpng.

References:
http://www.libpng.org/pub/png/libpng.html
http://scary.beasts.org/security/CESA-2004-001.txt
http://bugzilla.mozilla.org/show_bug.cgi?id=251381

- **Opera Browser "location" Object Write Access Vulnerability**

“Cross-site scripting attacks”

GreyMagic has discovered a vulnerability in Opera, allowing a malicious website to steal sensitive information and conduct cross-site scripting attacks.

The vulnerability is caused due to universal write access being enabled on the "location" object. This can be exploited by replacing methods in this object making it possible for a malicious website to override cross-site scripting restrictions for any website or local file.

The vulnerability has been reported in version 7.53 and prior.

References:
http://www.greymagic.com/security/advisories/gm008-op/

- **MailEnable Content-Length Denial Of Service Vulnerability**

“Remote denial of service”

MailEnable is reported prone to a remote denial of service vulnerability. This vulnerability is reported to exist in the MailEnable HTTP header parsing code.

When reading a large content-length header field from an HTTP request, the operation overflows a fixed size memory buffer and the HTTP service will reportedly crash.

The vulnerability can be exploited to crash the affected HTTP service, denying service to legitimate users. The possibility to execute arbitrary code may also be present.

References:
http://securityfocus.com/bid/10838/info/

- **PuTTY Authentication Process Buffer Overflow Vulnerabilities**

“Heap-based buffer overflow”

Core Security Technologies has discovered two vulnerabilities in PuTTY, which potentially can be exploited by malicious people to compromise a user's system.

1) A boundary error within the "modpow()" function can be exploited by passing an overly large value as a base for the modular exponentiation. This can e.g. be exploited during the initial SSH2 key exchange to cause a heap-based buffer overflow by sending a specially crafted packet.

Successful exploitation may allow execution of arbitrary code on a user's system but requires that a user has been tricked into connecting to a malicious server or a session can be intercepted in a MitM (Man-in-the-Middle) attack.

2) A boundary error within the "rsaencrypt()" function can e.g. be exploited during SSH1 key exchange to cause a heap-based buffer overflow by sending a specially crafted packet with a very small public key modulus.

Successful exploitation crashes the application but may potentially also allow execution of arbitrary code on a user's system. This requires that a user has been tricked into connecting to a malicious server or a session can be intercepted in a MitM (Man-in-the-Middle) attack.

The vulnerabilities affect version 0.54 and prior.

References:
http://www.chiark.greenend.org.u.../putty/wishlist/vuln-modpow.html
http://www.chiark.greenend.org.u...utty/wishlist/vuln-ssh1-kex.html
http://www.coresecurity.com/comm...oc.php?idx=417&idxseccion=10

- **SGI IRIX CDE Multiple Vulnerabilities**

“Gain escalated privileges”

SGI has confirmed multiple vulnerabilities in CDE, which can be exploited by malicious people to compromise a vulnerable system or gain escalated privileges.

References:
ftp://patches.sgi.com/support/fr...ity/advisories/20040801-01-P.asc

- **NetScreen ScreenOS SSHv1 Denial of Service Vulnerability**

"Denial of Service"

Mark Ellzey Thomas has discovered a vulnerability in ScreenOS, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in the handling of pre-authentication SSHv1 traffic.

Successful exploitation causes a vulnerable device to reboot or hang but requires that SSHv1 support is enabled.

References:
http://www.juniper.net/support/security/alerts/screenos-sshv1-2.txt

- **Mozilla / Netscape SOAPParameter Integer Overflow Vulnerability**

"Integer overflow"

zen-parse has reported a vulnerability in Mozilla and Netscape, potentially allowing malicious people to compromise a vulnerable system.

The vulnerability is caused due to an integer overflow within the SOAPParameter object's constructor. This can e.g. be exploited via a malicious web page containing specially crafted javascript.

This has been reported in Mozilla 1.6, and Netscape 7.0 and 7.1. Prior versions may also be affected.

References:
http://www.idefense.com/applicat...?id=117&type=vulnerabilities

- **Horde IMP Script Insertion Vulnerability**

"Script insertion attacks"

A vulnerability has been discovered in Horde IMP, which can be exploited by malicious people to conduct script insertion attacks.

The vulnerability is caused due to an input validation error in the HTML viewer and is reportedly a variant of an older vulnerability (see "Other References" section) reported by GreyMagic in Hotmail's and Yahoo's web-based email services.

Successful exploitation allows execution of arbitrary HTML and script code in a user's browser session when a malicious email is viewed.

References:
http://cvs.horde.org/diff.php/im....106&r2=1.389.2.109&ty=h

- **Citadel/UX Username Buffer Overflow Vulnerability**

"Buffer overrun"

A buffer overrun vulnerability is reported for Citadel/UX. The problem occurs due to insufficient bounds checking when processing 'USER' command arguments.

An anonymous remote attacker may be capable of exploiting this issue to execute arbitrary code. This however has not been confirmed. Failed exploit attempts may result in a denial of service.

References:
http://www.nosystem.com.ar/advisories/advisory-04.txt
http://securityfocus.com/bid/10833/info/

- **Microsoft Internet Explorer Multiple Vulnerabilities**

“Denial of Service, or compromise a user's system”

Microsoft has issued an update for Internet Explorer. This fixes three vulnerabilities, allowing malicious websites to cause a DoS (Denial of Service) or compromise a user's system.

1) An error can be exploited to bypass the zone restrictions in Internet Explorer.

2) An integer signedness error within the handling of BMP images can be exploited to execute arbitrary code. This vulnerability has already been fixed in prior service packs for Internet Explorer.

3) A boundary error within the handling of GIF images can reportedly be exploited to execute arbitrary code on a vulnerable system.

References:
http://www.microsoft.com/technet/security/bulletin/ms04-025.mspx

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