netVigilance

ScoutNews Team **29 October 2004**
Issue #44

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

2004's status as the year of the worms is being reassured with Beagle.BC growing as rapidly as MyDoom did.
The stock markets darling, Google is experiencing the marvels of technology as flaws wire their head at the public.
This week law enforcement has cranked down on some major internet crime rings excelling in SPAM as well as Identity theft.

Enjoy reading

Top Security News Stories this Week

❖ New Internet worm spreading quickly: experts

A new Internet worm was spreading quickly, threatening to overload computer systems around the world by generating copies by e-mail, security experts said.
"The Bagle.BC worm is increasing its already high rate of propagation, causing more and more incidents in users' computers worldwide," Panda said.
http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=6&u=/afp/20041029/tc_afp/internet_virus&sid=96001018
Technology - AFP

❖ Gmail accounts 'wide open to exploit'

Google's high profile webmail service, Gmail, is vulnerable to a security exploit that might allow hackers full access to a user's email account simply by knowing the user name, according to reports. The security flaw allows full access to users' accounts, with no need of a password, Israeli news site Nana says.
http://www.neowin.net/comments.php?id=25280&category=main
Deren Smith

❖ Feds Indict 19 on Online ID Theft Charges

Federal authorities have indicted 19 people in the United States and abroad on charges related to a Web site investigators claimed was one of the largest online centers for trafficking in stolen identity information and credit cards.
More than 20 others have also been charged in the probe.
The site, www.shadowcrew.com, had about 4,000 members who dealt with at least 1.7 million stolen credit card numbers and caused more than $4 million in losses, the Justice

Department said Thursday.
http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738&e=2&u=/ap/20041029/ap_on_hi_te/identity_theft
Jeffrey Gold

New Vulnerabilities Tested in SecureScout

- **19299 Hijack SafeguardProtect**
  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 Links: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/s/safeguardprotect.asp

- **19300 Hijack SafeSearch**
  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 Links: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/s/safesearch.asp

- **19301 Hijack SearchCentrix**
  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 Links: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/s/searchcentrix.asp

- **19302 Hijack SearchCentrix.ExpandSearch**

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/s/searchcentrix_expandsearch.asp

❖ **19303 Hijack SearchCentrix.Mygeek.com**

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/s/searchcentrix_mygeek_com.asp

❖ **19304 Hijack SearchCentrix.Search-O-Matic**

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/s/searchcentrix_search-o-matic.asp

❖ **19305 Hijack SearchCentrix.Webalize**

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/s/searchcentrix_webalize.asp

- **19306 Hijack SearchCentrix.WinDirect**
  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/s/searchcentrix_windirect.asp

- **19307 Hijack Searchex**
  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/s/searchex.asp

- **19308 Hijack SearchV**
  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/s/searchv.asp

New Vulnerabilities found this Week

- **MailCarrier HELO/EHLO Buffer Overflow Vulnerability**
  "Execution of arbitrary code"
  muts has discovered a vulnerability in MailCarrier, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of "HELO" and "EHLO" commands. This can be exploited to cause a buffer overflow by supplying an overly long argument.
Successful exploitation allows execution of arbitrary code.
The vulnerability has been confirmed on version 2.51. Other versions may also be affected.
NOTE: Exploit code is available.
References: http://secunia.com/advisories/12999/

- **Libxml2 Multiple Buffer Overflows**
  "Buffer Overflows"

infamous41md has reported a vulnerability in Libxml2, which potentially can be exploited by malicious people to compromise a vulnerable system.
1) The vulnerability is caused by a boundary error in the parsing of URLs with ftp information because user supplied data is copied into a fixed size buffer. This can potentially be exploited by malicious people by sending malicious XML documents to applications using the vulnerable part of the Libxml2 code.
2) The vulnerability is caused by a boundary error in the parsing of proxy URLs with ftp information because user supplied data is copied into a fixed size buffer. This can potentially be exploited by malicious people by sending malicious XML documents to applications using the vulnerable part of the Libxml2 code.
3) The vulnerability is caused by various boundary errors in the handling of DNS replies. This can potentially be exploited by malicious people by sending malicious DNS replies to applications using the vulnerable part of the Libxml2 code.
These vulnerabilities has been reported in libxml2-2.6.13 and libxml2-2.6.12. Other versions may also be vulnerable.
References: http://secunia.com/advisories/13000/

- **Quicktime Two Vulnerabilities**
  "Execute arbitrary code"

Two vulnerabilities have been reported in QuickTime, which can be exploited by malicious people to compromise a user's system.
1) An unspecified integer overflow can be exploited to cause a buffer overflow and execute arbitrary code on a user's system via a specially crafted HTML document.
This vulnerability only affects Windows systems.
2) A boundary error within the decoding of BMP images can be exploited to cause a heap-based buffer overflow and execute arbitrary code on a user's system.
This vulnerability affects both Windows and Mac OS X systems. However, it has been fixed priorly in Security Update 2004-09-30 for Mac OS X.
References:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0926
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0988

- **Horde "Help Window" Cross-Site Scripting Vulnerability**
  "Cross-site scripting attacks"

A vulnerability has been reported in Horde Application Framework, which potentially can be exploited by malicious people to conduct cross-site scripting attacks.
Input passed to the "help window" 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 vulnerability has been reported in version 2.2.6. Other versions may also be affected.
References: http://lists.horde.org/archives/announce/2004/000107.html

- **RealPlayer/RealOne "DUNZIP32.dll" Buffer Overflow Vulnerability**
  "Buffer overflow via a specially crafted skin file"

eEye Digital Security has reported a vulnerability in RealPlayer and RealOne, which potentially can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a boundary error in a 3rd-party compression library (DUNZIP32.dll) when processing skin files. This can be exploited to cause a buffer overflow via a specially crafted skin file.
Successful exploitation allows execution of arbitrary code.
The vulnerability affects the following versions:
* RealPlayer 10.5 (prior to build 6.0.12.1056)
* RealPlayer 10
* RealOne Player v2
* RealOne Player v1
References: http://www.service.real.com/help/faq/security/041026_player/EN/

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