netVigilance

ScoutNews Team **25 June 2004**
Issue #26

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

We thought we were being hoaxed when doing the final research for ScoutNews today, but it seems to be a real threat coming on to the internet based on some undocumented vulnerability in IIS v 5.0. If this is in fact **Download.Ject** the danger is not too big and you can read:
http://www.microsoft.com/security/incident/download_ject.mspx
If it is something else the impact could be dangerous and of a magnitude that will dominate our lives months to come.

In other news there is a new report out claiming that we are using low cost outsourced labor to develop automated intelligent SW that in turn will have a much bigger impact on the job loss in the western world.

….and: Yes, it is illegal to use the Internet to perform fraudulent activities.

Enjoy reading

Top Security News Stories this Week

❖ **Californian charged over 'Google-defrauding' software**
A California man was arraigned on Thursday on federal extortion and wire fraud charges arising from a software program that he claimed could allow spammers to defraud Web search company Google of millions of dollars, federal prosecutors said.
http://news.zdnet.co.uk/business/legal/0,39020651,39158639,00.htm
Reuters

❖ **Mainstream Web sites spreading back-door infections**
Security researchers warned Web surfers on Thursday to be on their guard after uncovering evidence that widespread Web server compromises have turned corporate home pages into points of digital infection.
The researchers believe that online organized crime groups are breaking into Web servers, surreptitiously inserting code that takes advantage of two flaws in Internet Explorer that Microsoft has not yet fixed. Those flaws allow the Web server to install a program that takes control of the user's computer.

http://news.zdnet.co.uk/internet/security/0,39020375,39158636,00.htm
Robert Menos

❖ Intelligent systems 'will take more jobs than outsourcing'

Smart applications that automate jobs in areas such as customer service, helpdesk and directory assistance will cause more job cuts than outsourcing, according to a new report

In the coming years, a large number of first-level jobs in service industries related to customer service, help desk and directory assistance will be lost due to the advent of intelligent systems, research firm Strategy Analytics said in the report.

http://news.zdnet.co.uk/business/employment/0,39020648,39158759,00.htm
CNET News

❖ Internet websites under attack? Microsoft issues advice to website owners and internet surfers

Following several media reports of many websites being affected by a new piece of malware known as JS/Scob-A (also know as Download.Ject or Toofer), Microsoft has published advice to both corporate and home users.

Scob appears to affect websites running Microsoft IIS 5.0 and has been found appending its malcious section of JavaScript code into HTML webpages. Websites running latest versions of Microsoft IIS, or who use web software from other vendors, do not appear to be affected.

If users of Internet Explorer visit webpages infected by Scob, their computer may attempt to download a file from a Russian website. Currently the website is unavailable.

http://www.sophos.com/virusinfo/articles/scobalert.html
Sophus

❖ Major Internet Attack Under Way

Internet security organizations are warning that dozens of major Internet sites, and potentially thousands of Web sites across the Internet, are currently under attack. Several Web administrators from major companies said their Windows-based Web servers were compromised despite being up to date on security patches, security analysts reported.

"We've been watching activity since last Sunday, but it's now hit a critical mass," says Marcus Sachs, director of the SANS Internet Storm Center, who is in communications with Homeland Security's National Cyber Security division about the attack.

http://www.securitypipeline.com/news/22102093;jsessionid=LNBS2ZJ4RFCKSQSNDBCSKHQ
George V. Hulme

New Vulnerabilities Tested in SecureScout

➢ 13107 CVS Multiple Vulnerabilities

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

Multiple vulnerabilities have been reported in CVS, which can be exploited by malicious users to cause a DoS (Denial of Service) or compromise a vulnerable system.

1) An NULL-termination error within the patch for the previous "Entry" line heap-based buffer overflow vulnerability can potentially be exploited to crash a vulnerable server.

2) A "double free" error can reportedly be exploited via the "Argumentx" command to execute arbitrary code on a vulnerable system.

3) A format string error within the processing of the CVS wrapper file can potentially be exploited to execute arbitrary code on a vulnerable system by including a specially crafted line containing format specifiers. However, successful exploitation requires CVSROOT commit access.

4) An integer overflow within the handling of the "Max-dotdot" CVS protocol command can be exploited to crash the CVS server and consume available disk space.

5) An boundary error within the "serve_notify()" function when handling empty data lines can potentially be exploited to execute arbitrary code.

6) Some underflow errors exist when reading configuration files containing empty lines from CVSROOT. Successful exploitation requires CVSROOT commit access, and the impact is unknown.

7) Various integer multiplication overflows may potentially be exploited for arbitrary code execution.

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

CVE Links: CAN-2004-0414 & CAN-2004-0416 & CAN-2004-0417 & CAN-2004-0418

Reference: https://ccvs.cvshome.org/servlets/ProjectDownloadList

➢ 13108 CVS Entry Line Heap Overflow Vulnerability

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

The vulnerability is caused due to a boundary error within the handling of modified or unchanged flag insertion into CVS entry lines, which can be exploited to cause a heap overflow.

Successful exploitation allows execution of arbitrary code.

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

CVE Links: CAN-2004-0396

Reference: http://ccvs.cvshome.org/servlets/ProjectDownloadList

➢ 13129 CVS Path Validation Vulnerabilities

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

Two vulnerabilities have been discovered in CVS. These can be exploited by malicious servers to compromise clients and by malicious users to retrieve arbitrary files from a vulnerable server.

1) Missing validation of paths within CVS clients makes it possible to create RCS diff files with absolute paths. This may allow creation or overwriting of files in arbitrary locations on a user's system.

Successful exploitation requires that a user is tricked into connecting to a malicious CVS server.

2) An error in the server makes it possible for users to request the content of arbitrary RCS archive files above $CVSROOT.

Test Case Impact: **Gather Info** Vulnerability Impact: **Remote Execution** Risk: **High**

CVE Link: CAN-2004-0180

Reference: https://ccvs.cvshome.org/servlets/ProjectDownloadList

➢ 14364 CheckMail Disclosing Passwords to Local Users Vulnerability

CheckMail 1.2 stores account information, including usernames and passwords of email accounts, in a registry keys.
This allow any remote attacker to disclose sensitive information in order to perform further serious actions.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.securitytracker.com/alerts/2003/Aug/1007517.html & http://www.desksoft.com

➢ 15007 Microsoft IIS 2 & 3 ASP Appended Dot Vulnerability

Appending a period (.) to an ASP URL will send the unprocessed ASP, revealing source code. This is a major issue, because the source code often contains login information (e.g. database access).
For example, http://server_name/asp_directory/file.asp becomes http://server_name/asp_directory/file.asp. (with .).

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

CVE Link: CAN-1999-0154

Reference: http://ciac.llnl.gov/ciac/bulletins/h-48.shtml & http://pulhas.org/xploitsdb/NT/asp.html & http://support.microsoft.com/support/kb/articles/Q163/4/85.asp

➢ 15008 Microsoft IIS3 ASP %2e Source Disclosure Vulnerability

Using URLs such as http://.../default%2easp may reveal ASP code, instead of executing.

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

CVE Link: CAN-1999-0253

Reference: http://www.securityfocus.com/bid/1814

➢ 15050 Fingerd Enabled

The finger daemon gives away information on a user that should be restricted to other individuals working very closely with the given user, including:
- if the user is logged on to the system;
- how long the connection from which he accesses the system has been idle;
- his "home directory" and other information;
- occasionally his schedule.
It is very dangerous to release this information in an environment where security is an issue.

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

CVE Link: CVE-1999-0612

Reference: http://www.cert.org/advisories/CA-1993-04.html

➢ 15773 GlimpseHTTP and WebGlimpse Piped Command Vulnerability

Some versions of the a glimpse CGI script (part of the GlimpseHTTP or WebGlimpse packages, used in indexing and querying web sites) are vulnerable to an attack that leads to possible remote command execution.
This test has found a glimpse on the web server, but cannot determine if the running version is vulnerable or not.

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

CVE Link: CVE-1999-0147

Reference: http://www.cert.org/vendor_bulletins/VB-97.13.GlimpseHTTP.WebGlimpse & http://webglimpse.org/security.html

➢ 17485 Cisco Catalyst 2900 Switch Webserver Denial Of Service Vulnerability

Cisco Catalyst 2900 Switches can be remotely administrated through the webserver

embedded in those switches. This web console allows remote attackers to cause a denial of service via a flood of invalid login requests to the web service, which do not properly disconnect the user after several failed login attempts.
This results in a denial of service of the device preventing users from connecting to this administrative service.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: www.Cisco.com

➢ 17904 Linksys remote HTTP management Admin access Vulnerability

Linksys is known as the leader in networking solutions for the home and small business particularly wireless LAN equipment, broadband routers, network adapters for the desktop and notebook PC and hubs and switches.

Linksys routers provide an HTTP remote management interface.

The router is using the default factory configuration, and can be administered remotely, using the default password "admin".

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: www.Linksys.com

New Vulnerabilities found this Week

❖ Internet Explorer Local Resource Access and Cross-Zone Scripting Vulnerabilities

« local resource access ; execute files in the "Local Machine" security zone »

Two vulnerabilities have been reported in Internet Explorer, which in combination with other known issues can be exploited by malicious people to compromise a user's system.

1) A variant of the "Location:" local resource access vulnerability can be exploited via a specially crafted URL in the "Location:" HTTP header to open local files.

Example:
"Deleted"

2) A cross-zone scripting error can be exploited to execute files in the "Local Machine" security zone.

Secunia has confirmed the vulnerabilities in a fully patched system with Internet Explorer 6.0. It has been reported that the preliminary SP2 prevents exploitation by denying access.

Successful exploitation requires that a user can be tricked into following a link or view a malicious HTML document.

NOTE: The vulnerabilities are actively being exploited in the wild to install adware on users' systems.

CAN-2004-0549

References: http://archives.neohapsis.com/ar...fulldisclosure/2004-06/0104.html & http://www.kb.cert.org/vuls/id/713878

❖ IBM Access Support ActiveX Controls Various Insecure Methods

« place a file in an arbitrary location »

eEye Digital Security has reported some vulnerabilities in two IBM Access Support ActiveX controls, which potentially can be exploited by malicious people to compromise a user's system.

1) The IBM acpRunner Access Support ActiveX control includes some insecure methods ("DownLoadURL", "SaveFilePath", and "Download"), which allow a malicious web site to place a file in an arbitrary location on a user's system.

2) IBM eGatherer Access Support ActiveX control also includes some insecure methods ("GetMake", "GetModel", "GetOSName", "SetDebugging", and "RunEgatherer"), which may allow a malicious web site to place a file in an arbitrary location on a user's system.

The ActiveX controls are reportedly installed by default on many IBM PC models.

References:http://www.eeye.com/html/research/advisories/AD20040615A.html & http://www.eeye.com/html/research/advisories/AD20040615B.html

❖ 3Com SuperStack Switches HTTP Request Denial of Service

« Denial of Service »

A vulnerability has been discovered in various 3Com SuperStack switches, allowing malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error within the handling of requests for the WEB management interface. This can reportedly be exploited to reset a vulnerable device via specially crafted requests.

The following products are affected:
* SuperStack 3 Switch 4400 (3C17203, 3C17204)
* SuperStack 3 Switch 4400 SE (3C17206)
* SuperStack 3 Switch 4400 PWR (3C17205)
* SuperStack 3 Switch 4400 FX (3C17210)

References: http://secunia.com/advisories/11934/

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