netVigilance

ScoutNews Team **March 4, 2005**
Issue # 9

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Hackers tap cell phone voicemail boxes, hackers use sniper rifle to pick off cell phones of RSA attendees and lax security can extract hidden costs for banks and ecommerce.

Enjoy

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **T-mobile hack exposes user's voice mailboxes.**

Hackers can gain access to t-mobile user voice mailboxes simply using the victim's cell phone number. It is reported that hackers can listen to the victim's voice mail, take control of the victim's voice mail functions, record the voice mail to a file on a remote server, and also make calls out from the system posing as the victim.

T-mobile users are advised to set password protection on voice mail functions to prevent getting hacked.

CNET News.com

Full Story : http://news.zdnet.com/2100-1009_22-5589608.html

- **Bluetooth sniper rifle, picks off cell phone users at RSA Conference.**

A group of hackers from the wireless think tank Flexilis, constructed a Bluetooth sniper rifle to hack cellphones for less than $500 in parts.

The 'rifle; consists of a Bluetooth antennae, rifle stock and a gumstick computer as the magazine. According to Kevin Mahaffey, the main programmer at Flexilis; the device can perform vulnerability and service scans, crash or even rip contact lists from vulnerable phones.

Tom's hardware guide

Full Story: http://www.tomshardware.com/hardnews/20050217_180417.html

- **Forrester Research analyst forecasts business erosion for corporations that do not make security top priority.**

Jonathan Penn of Forrester Research describes a growing consumer trend to shy away from online transactions for fear of identity theft. The Forrester data indicates that 92% of those polled, are reluctant to share personal information online.

Record numbers for online purchases during the '04 holiday buying season has brought more attention by hackers to exploit this market. Phising activity also saw it's greatest increase in January '05, 47% over December. (*related sites*: http://www.ecommercetimes.com/rsstory/41015.html , http://www.antiphishing.org/)

Forrester estimates that loss of business could run into the trillions of dollars for banks and ecommerce businesses that do not instill customer confidence in the handling of their personal information.

SecurityNewsPortal

Full Story: http://www.snpx.com/cgi-bin/news55.cgi?target=87004656?-2622

New Vulnerabilities Tested in SecureScout

- **14475 W32/Bagle.bl Worm (Registry Check)**

This is a mass-mailing worm with the following characteristics:

contains its own SMTP engine to construct outgoing messages
harvests email addresses from the victim machine
the From: address of messages is spoofed

contains a remote access component (notification is sent to hacker)
copies itself to folders that have the phrase shar in the name (such as common peer-to-peer applications; KaZaa, Bearshare, Limewire, etc)

Messages are constructed as follows

From : (address is spoofed)
Subject :

Delivery service mail
Delivery by mail
Registration is accepted
Is delivered mail
You are made active

Body Text:

Thanks for use of our software.
Before use read the help

Attachment: (may be one of the following, with an extension of .exe, .scr, .com, or .cpl)

wsd01
viupd02
siupd02
guupd02
zupd02
upd02
Jol03

The virus copies itself into the Windows System directory as sysformat.exe. For example:

C:\WINNT\SYSTEM32\sysformat.exe

It also creates other files in this directory to perform its functions:

C:\WINNT\SYSTEM32\sysformat.exeopen
C:\WINNT\SYSTEM32\sysformat.exeopenopen

Method of Infection

Mail Propagation

This virus constructs messages using its own SMTP engine. Target email addresses are harvested from files on the victim machine.

Peer To Peer Propagation

Files are created in folders that contain the phrase shar.

Remote Access Component

The virus listens on random TCP ports, for remote connections. It attempts to notify the author that the infected system is ready to accept commands, by contacting various websites, calling a JPG file (error.jpg) on the remote sites.

TC Impact: Gather Info

Test Method: Check if the "sysformat" REG_SZ exists under the following registry key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

If the REG_SZ does not exist then issue a NOTFOUND.
If can not access the registry key then issue an UNKNOWN.
If exists then continue with:

Check if the REG_SZ value contains "sysformat.exe" using a non case sensitive function.
("sysformat" = C:\WINNT\SYSTEM32\sysformat.exe)

If can not read value then issue a UNKNOWN.
If the values matches then the target is vulnerable.

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

References:
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=131353

CVE Reference: GENERIC-MAP-NOMATCH

❖ **14476 W32/Bagle.bn Worm (Registry Check)**

This is a mass-mailing worm with the following characteristics:

* contains its own SMTP engine to construct outgoing messages
* the From: address of messages is spoofed
* attachment may be a password-protected zip file, with the password included in the message body
* contains a remote access component (notification is sent to hacker)
* uses various mutex names selected from those W32/Netsky variants have used, in order to prevent those W32/Netsky variants running on infected machines
* deletes registry entries of security programs and other worms

** Messages are constructed as follows **
The details are as follows:

From : (address is spoofed)
Subject : (blank)

Body Text:

* Password:
* Pass -
* Password -
* new price
* price
* The password is
* Password:

Attachment:

* price.zip
* price2.zip
* price_new.zip
* price_08.zip
* 08_price.zip
* newprice.zip
* new_price.zip
* new__price.zip

Within the ZIP file is an executable file named doc_01.exe.

The virus copies itself into the Windows System directory as windlhhl.exe.
For example:

* C:\WINDOWS\SYSTEM32\windlhhl.exe

** Method of Infection

** Mail Propagation

This virus constructs messages using its own SMTP engine. It may try to download a file which contains a list of email addresses to send to, but at the time of writing this file was unavailable.

** Remote Access Component

The virus listens on TCP port 80 for remote connections. It attempts to open a file, script1.php, on the localhost.

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

References:
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=132120

CVE Reference: GENERIC-MAP-NOMATCH

❖ **14477 W32/Bagle.bn Worm (Registry Check)**

This is a mass-mailing worm with the following characteristics:

* contains its own SMTP engine to construct outgoing messages
* harvests email addresses from the victim machine
* the From: address of messages is spoofed
* contains a remote access component (notification is sent to hacker)
* copies itself to folders that have the phrase shar in the name (such as common peer-to-peer applications; KaZaa, Bearshare, Limewire, etc)

** Messages are constructed as follows **
From : (address is spoofed)
Subject :

* Delivery service mail
* Delivery by mail
* Registration is accepted
* Is delivered mail
* You are made active

Body Text:

* Thanks for use of our software.
* Before use read the help

Attachment: (may be one of the following, with an extension of .exe, .scr, .com, or .cpl)

* wsd01
* viupd02
* siupd02

* guupd02
* zupd02
* upd02
* Jol03

The virus copies itself into the Windows System directory as sysformat.exe. For example:

* C:\WINNT\SYSTEM32\sysformat.exe

It also creates other files in this directory to perform its functions:

* C:\WINNT\SYSTEM32\sysformat.exeopen
* C:\WINNT\SYSTEM32\sysformat.exeopenopen

** Method of Infection

** Mail Propagation

This virus constructs messages using its own SMTP engine. Target email addresses are harvested from files on the victim machine.

** Remote Access Component

The virus listens on random TCP ports, for remote connections. It attempts to notify the author that the infected system is ready to accept commands, by contacting various websites, calling a JPG file (error.jpg) on the remote sites.

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

References:
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=131352

CVE Reference: GENERIC-MAP-NOMATCH

❖ **15166 Mozilla / Firefox / Thunderbird Multiple Vulnerabilities (Remote File Checking)**

Details have been released about several vulnerabilities in Firefox, Mozilla and Thunderbird. These can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges and by malicious people to conduct spoofing attacks, disclose and manipulate sensitive information, and potentially compromise a user's system

1) The vulnerability is caused due to the temporary plugin directory being created insecurely. This can be exploited via symlink attacks to delete arbitrary directories with the privileges of the user running Mozilla or Firefox.

2) The problem is that an inactive tab can launch an HTTP authentication prompt, which appears to be displayed by a website in another tab. This may be exploited to trick a user into entering some sensitive information (e.g. user credentials).

3) An error in the handling of shortcut files (.lnk) can be exploited to overwrite arbitrary files by tricking a user into downloading a shortcut file twice.

4) The problem is that a XML document can include XSLT stylesheets from arbitrary sites, which may be exploited to disclose some sensitive information.

5) An error in the form fill feature (autocomplete) allows reading suggested values before they are chosen. This can be exploited to disclose some potentially sensitive input by tricking a user into arrowing through some autocompleted values.

6) A memory handling error in Mozilla string classes may allow overwriting of memory if the browser runs out of memory during string growth. This can potentially be exploited to execute arbitrary code.

7) The problem is that the hostname can be obfuscated in the installation confirmation dialog by including an overly long username and password. This can be exploited to trick users into accepting installations from untrusted sources.

Successful exploitation requires that the malicious website is allowed to request installations.

8) It is possible to cause a heap overflow due to an error when converting malformed UTF8 character sequences to Unicode. This may be exploited to cause a heap overflow and execute arbitrary code, however, general web content is not converted using the vulnerable code.

9) Various errors make it possible to show the "secure site" lock icon with certificate information belonging to a different site.

Mozilla 1.7.6, Firefox 1.0.1and Thunderbird 1.0.1 fix the issue.

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

References:

Original Advisory:

http://www.idefense.com/application/poi/display?id=200&type=vulnerabilities

http://www.mozilla.org/security/announce/mfsa2005-28.html

http://www.mozilla.org/security/announce/mfsa2005-24.html

http://www.mozilla.org/security/announce/mfsa2005-21.html

http://www.mozilla.org/security/announce/mfsa2005-20.html

http://www.mozilla.org/security/announce/mfsa2005-19.html

http://www.mozilla.org/security/announce/mfsa2005-18.html

http://www.mozilla.org/security/announce/mfsa2005-17.html

http://www.mozilla.org/security/announce/mfsa2005-15.html

http://www.mozilla.org/security/announce/mfsa2005-14.html

Other References:

http://secunia.com/advisories/12712/

Product HomePage:

http://www.mozilla.org/products/mozilla1.x/

http://www.mozilla.org/products/firefox/

http://www.mozilla.org/projects/thunderbird/

CVE Reference: CAN-2005-0255 CAN-2005-0578 CAN-2005-0584 CAN-2005-0587 CAN-2005-0588 CAN-2005-0589 CAN-2005-0590 CAN-2005-0592 CAN-2005-0593

- **15167 Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting (Remote File Checking)**

Paul has reported a vulnerability in Mozilla Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks.

The vulnerability is caused due to missing URI handler validation when dragging an image with a "javascript:" URL to the address bar. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site by tricking a user into dragging an image to the address bar.

This is similar to vulnerability 2 in:
SA14160

The vulnerability has been reported in version 1.0 and 1.0.1. Other versions may also be affected.

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

References:

Original Advisory:

Other References:

http://secunia.com/advisories/14160/

Product HomePage:

http://www.mozilla.org/products/firefox/

CVE Reference: none.

❖ **15168 Mozilla / Firefox "Save Link As" Download Dialog Spoofing (Remote File Checking)**

Secunia Research has discovered a vulnerability in Mozilla and Mozilla Firefox, which can be exploited by malicious people to trick users into downloading malicious files.

The problem is that the browser uses the URL to determine the file type association in the "Save Link As" download dialog, but uses the filename from the "Content-Disposition" HTTP header when saving the downloaded file. This can be exploited by a malicious web site to spoof file types in the "Save Link As" download dialog.

Successful exploitation can lead to malware being saved to the download directory (default is the desktop on Mozilla Firefox).

NOTE: Exploitation requires that the option "Hide extension for known file types" is enabled in Windows (default setting).

The vulnerability has been confirmed in Mozilla 1.7.3 and Mozilla Firefox 1.0 for Windows. Other versions may also be affected.

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

References:

Original Advisory:

http://secunia.com/secunia_research/2004-21/advisory/

http://www.mozilla.org/security/announce/mfsa2005-22.html

Product HomePage:

http://www.mozilla.org/products/firefox/

CVE Reference: CAN-2005-0586

❖ **16008 WU-FTPD Wildcard Denial of Service Vulnerability**

Adam Zabrocki has reported a vulnerability in WU-FTPD, which can be exploited by malicious users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the handling of "ls" queries with multiple wildcard chars (*). This causes WU-FTPD to consume large

amounts of CPU resources and may cause the system to become unresponsive by issuing multiple queries simultaneously.

The vulnerability has been reported in versions 2.6.1 and 2.6.2. Prior versions may also be affected.

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

References:

Original advisory:

http://www.idefense.com/application/poi/display?id=207&type=vulnerabilities

Product page:

http://www.wu-ftpd.org

CVE Reference: CAN-2005-0256

❖ **16009 WU-FTPD Directory Access Restriction Bypass Vulnerability**

Glenn Stewart has discovered a vulnerability in wu-ftpd, which can be exploited by malicious, authenticated users to circumvent certain restrictions.

A user can reportedly bypass the directory access restrictions imposed by the "restricted-gid" option by changing the permissions on their home directory using chmod. This will cause wu-ftpd to fall back to the root directory on subsequent logins when access to the user's home directory is denied.

The issue affects wu-ftpd 2.6.2 and earlier.

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

References:

Original advisory:

http://www.linuxsecurity.com/content/view/118059/98/

Other references:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0148

http://www.sco.com/support/security/index.html

http://www.sco.com/support/forums/security.html

Product page:

http://www.wu-ftpd.org

CVE Reference: CAN-2004-0148

❖ 16010 WU-FTPD S/KEY Authentication Buffer Overflow Vulnerability

A vulnerability has been reported in WU-FTPD, which potentially can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the S/KEY challenge handling. This can be exploited by supplying overly long, specially crafted user credentials, which causes a buffer overflow and may allow execution of arbitrary code.

Successful exploitation requires that S/KEY authentication has been enabled.

The vulnerability was originally reported in version 2.6.0 in June 2000, but has now also been reported to affect the latest version (2.6.2).

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

References:

Original advisory:

http://www.securiteam.com/unixfocus/6X00Q1P8KC.html

Other references:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0185

Product page:

http://www.wu-ftpd.org

CVE Reference: CAN-2004-0185

❖ 16011 RealPlayer WAV and SMIL File Handling Buffer Overflows (Remote File Checking)

Four vulnerabilities have been reported in Cisco Application and Content Networking System (ACNS), which can be exploited by malicious people to

cause a DoS (Denial of Service).

1) An error within the processing of TCP connections can be exploited to cause the ACNS cache process to restart.

2) An error within the processing of IP packets can be exploited to consume 100% CPU resources.

3) An error within the processing of network packets can be exploited to cause the RealServer RealSubscriber to consume 100% CPU resources.

4) An error within the processing of IP packets can be exploited to cause the device to continuously forward copies of a specially crafted packet.

The vulnerabilities affect devices configured as a transparent, forward, or reverse proxy server.

It has also been reported that the administrative account may contain a default password.

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

References:

Original advisory:

http://service.real.com/help/faq/security/050224_player/EN/

http://www.idefense.com/application/poi/display?id=209&type=vulnerabilities

Other references:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0455

CVE Reference: CAN-2005-0455

New Vulnerabilities found this Week

- **RealPlayer WAV and SMIL File Handling Buffer Overflows "Remote System access"**

  Two vulnerabilities have been reported in various RealNetworks products, which can be exploited by malicious people to compromise a user's system.

  1) A boundary error within the processing of WAV files can be exploited to cause a buffer overflow via a specially crafted WAV file.

2) A boundary error within the processing of SMIL files can be exploited to cause a stack-based buffer overflow via a specially crafted SMIL file.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

References
http://www.idefense.com/application/poi/display?id=209&type=vulnerabilities
http://service.real.com/help/faq/security/security022405.html
http://service.real.com/help/faq/security/050224_player/EN/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0455
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0611
http://secunia.com/advisories/14456/

- **PHPNews Arbitrary File Inclusion Vulnerability "Remote System access"**

Filip Groszynski has reported a vulnerability in PHPNews, allowing malicious people to compromise a vulnerable system.

Input passed to the "path" parameter in "auth.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.

Successful exploitation requires that "register_globals" is enabled.

The vulnerability has been reported in version 1.2.4.

References
http://newsphp.sourceforge.net/index.php?action=showcat&catid=2
http://secunia.com/advisories/14449/

- **WebMod "Content-Length" Buffer Overflow Vulnerability "Denial of Service / Remote System access"**

Kevin Masterson has reported a vulnerability in the WebMod plugin for Half-Life Dedicated Server, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of POST data in "server.cpp". This can be exploited to cause a heap-based buffer overflow by supplying more POST data than the value of the "Content-

Length" HTTP header.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been confirmed in version 0.47. Prior versions may also be affected.

References
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0608
http://djeyl.net/w.php
http://secunia.com/advisories/14302/

- **KNet HTTP Request Processing Buffer Overflow Vulnerability "Remote System access"**

CorryL has reported a vulnerability in KNet, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error when processing HTTP GET requests. This can be exploited to cause a buffer overflow by supplying an overly long GET request (about 522 bytes) to the server.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 1.04c. Other versions may also be affected.

References
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0575
http://secunia.com/advisories/14400/

- **Trend Micro Products AntiVirus Library Buffer Overflow "Remote System access"**

ISS X-Force has reported a vulnerability in various Trend Micro products, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the AntiVirus library when processing ARJ files. This can be exploited to cause a heap-based buffer overflow via a specially crafted ARJ file containing an overly long filename.

References
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0533

http://secunia.com/advisories/14396/

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