ScoutNews Team **April 26, 2005**
Issue # 16

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

The White Hats make a couple of charges; NSF grants, Phishing arrests. On the darker side; Sober is back, Carnegie-Mellon gets hacked and Zombies are spreading like – well, like Zombies in China.

Be Careful out there.

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

Top Security News Stories this Week

- **Sober Worm back in sneaky variant**

A new variant of the Sober Worm has emerged and is spreading fast. Sober-M employs harvesting to scour your email addresses and send these back to the anonymous author.

The list is exploited to further the spread of the Worm and is often sold to Spammers and Phishers.

The latest Sober attack uses the subject line: "I've_got your E-mail on my_account! " and broken English to seem authentic. Ensure that your Virus scanner is up to date and always be careful of opening suspicious email

messages.

Full Story:
http://www.zdnetindia.com/help/alerts/stories/120716.html

- **Cornell University lands portion of $19M NSF grant to study computer security.**

Chalk one up for the white hats. A research team made up of computer specialist, legal advisors and economics experts focusing on improvements to technology enabling stronger, more trustworthy infrastructures.

The consortium, Team for Research in Ubiquitous Secure Technology (TRUST); seeks to develop classroom curriculum aimed at addressing the relative vulnerability of some vital but often overlooked systems that our daily lives depend upon like: air traffic control, financial services, electrical power, etc.
The Cornell Daily Sun

Full Story :
http://www.cornellsun.com/vnews/display.v/ART/2005/04/20/4265f0f8d35b4

- **Carnegie-Mellon University Business school hacked.**

A Hacker broke into the computers of the Tepper School of Business; gaining access to social security numbers, credit card accounts and other personal data of about 6,000 people.

The hacker had access to records of current / former students, staff and applicants.
CBS

Full Story:
http://kdka.com/topstories/local_story_111102454.html

- **Zombies inundating China's internet**

The rapid growth of the internet in China is bringing with it an army of computers being solicited as Zombies being used in DoS, Spamming and Phishing. Of the 157,000 zombies that appear daily, 20% are in China

Hackers are targeting the emerging and relatively unprotected user community there.

IDG News Service

Full Story:
http://security.itworld.com/4340/050421zombies/page_1.html

- **Arizona Phishers busted**

Two men were arrested in Tuscon, Arizona charged with several counts of credit card theft, fraudulent schemes, and money laundering. The two men, age 24 and 19, were apparently running a Phishing scam where they would trick people out of their credit card information to make counterfeit cards.

Full Story:
http://www.techweb.com/wire/security/161500412

New Vulnerabilities Tested in SecureScout

- **13214 Oracle Database Server - Data Pump component unspecified error (apr-2005/DB03)**

  An unspecified error in the Data Pump component can potentially be exploited to disclose or manipulate information.

  Successful exploitation requires execute permissions on dbms_metadata.

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

  References:

  Original Advisory:
  http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
  http://www.ngssoftware.com/advisories/oracle-03.txt
  http://secunia.com/advisories/14935/

  Product Homepage:
  http://www.oracle.com/

  CVE Reference: None.

- **13215 Oracle Database Server - Intermedia component unspecified error (apr-2005/DB04)**

An unspecified error in the Intermedia component can potentially be exploited to disclose or manipulate information.

Successful exploitation requires execute permissions on ordsys.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

❖ 13216 Oracle Database Server - Authentication component unspecified error (apr-2005/DB05)

An unspecified error in the Authentication component can potentially be exploited to disclose or manipulate information.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

❖ 13217 Oracle Database Server - Database SSL Library component unspecified error (apr-2005/DB06)

An unspecified error in the Database SSL Library component can potentially be exploited to disclose or manipulate information.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

❖ 13218 Oracle Database Server - Internet Directory component unspecified error (apr-2005/DB07)

An unspecified error in the Internet Directory component can potentially be exploited to disclose or manipulate information.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

❖ 13219 Oracle Database Server - Spatial component unspecified error (apr-2005/DB08)

An unspecified error in the Spatial component can potentially be exploited to disclose or manipulate information.

Successful exploitation requires execute permissions on mdsys.prvt_idx.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

❖ 13220 Oracle Database Server - XML Database component unspecified error (apr-2005/DB09)

An unspecified error in the XML Database component can potentially be exploited to disclose or manipulate information.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

❖ 13221 Oracle Database Server - XDK component unspecified error (apr-2005/DB10)

An unspecified error in the XDK component can potentially be exploited to disclose or manipulate information.

Successful exploitation requires execute permissions on SYS_DBURIGEN.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **13222 Oracle Database Server - Oracle HTTP Server component unspecified error (apr-2005/DB12)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **13223 Oracle Database Server - Oracle HTTP Server component unspecified error (apr-2005/DB13)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

New Vulnerabilities found this Week

- **Realplayer/RealOne RAM File Processing Buffer Overflow Vulnerability**
"Buffer overflow; Execution of arbitrary code"

Piotr Bania has reported a vulnerability in Realplayer and RealOne, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when processing RAM files and can be exploited to cause a buffer overflow via a specially crafted RAM file.

Successful exploitation allows execution of arbitrary code.

The vulnerability affects the following products:
* RealPlayer 10.5 (6.0.12.1040-1059)
* RealPlayer 10
* RealOne Player v2
* RealOne Player v1
* RealPlayer 8
* RealPlayer Enterprise
* Mac RealPlayer 10 (10.0.0.305 - 331)
* Mac RealOne Player
* Linux RealPlayer 10 (10.0.0 - 3)
* Helix Player (10.0.0 - 3)

References:
http://service.real.com/help/faq/security/050419_player/
http://www.service.real.com/help/faq/security/security041905.html
http://pb.specialised.info/all/adv/real-ram-adv.txt

❖ **RaidenFTPD Unspecified Arbitrary File Access Vulnerability**

"Access arbitrary files outside the FTP root"

A vulnerability has been reported in RaidenFTPD, which can be exploited by malicious users to gain knowledge of sensitive information.

The vulnerability is caused due to an unspecified error and makes it possible to access arbitrary files outside the FTP root.

References:
http://forum.raidenftpd.com/showflat.php?Board=UBB13&Number=45685

❖ **Microsoft Windows Explorer Web View Script Insertion Vulnerability**

"Execute arbitrary HTML and script code"

GreyMagic has discovered a vulnerability in Windows, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an input validation error in the Web View library "webvw.dll" where certain metadata for files isn't properly sanitized before being used. This can be exploited to execute arbitrary HTML and script code in a local context with escalated privileges by e.g. tricking a user into selecting a malicious word document with a specially crafted author name in Windows Explorer.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been confirmed on a fully patched Microsoft Windows 2000 SP4 system.

References:
http://www.greymagic.com/security/advisories/gm015-ie/

- **MPlayer RTSP and MMST Streams Buffer Overflow Vulnerabilities**

"Execution of arbitrary code"

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

1) A boundary error when processing lines from RealMedia RTSP streams can be exploited to cause a heap-based buffer overflow via a specially crafted response with a large amount of lines.

Successful exploitation may allow execution of arbitrary code.

2) A boundary error when processing stream IDs from Microsoft Media Services MMST streams can be exploited to cause a heap-based buffer overflow via a specially crafted response with more than 20 stream IDs.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities have been reported in versions 1.0pre6 and prior.

References:
http://www.mplayerhq.hu/homepage/design7/news.html#vuln10
http://www.mplayerhq.hu/homepage/design7/news.html#vuln11

- **Sun Java System Web Proxy Server Unspecified Buffer Overflow**

"Execution of arbitrary code"

A vulnerability has been reported in Sun Java System Web Proxy Server, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified error and can be exploited to cause a buffer overflow.

Successful exploitation may allow execution of arbitrary code with the privileges of the server process (user "nobody" by default).

The vulnerability affects version 3.6 Service Pack 6 and prior.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57763-1

- **Simple Web Server Request Handling Buffer Overflow**

"Execution of arbitrary code"

Michael Thumann has reported a vulnerability in PMSoftware Simple Web Server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error when handling HTTP requests and can be exploited to cause a stack-based buffer overflow via an overly long HTTP GET request (about 260 bytes).

Successful exploitation allows execution of arbitrary code.

The vulnerability has been reported in version 1.015. Other versions may also be affected.

References:
http://secunia.com/advisories/15000/

- **Sun Solaris Network Port Hijacking Vulnerability**

"Hijack network ports"

A vulnerability has been reported in Solaris, which can be exploited by malicious, local users to hijack network ports.

The vulnerability is caused due to an unspecified error making it possible to bind a process to a non-privileged network port, which already has been bound (e.g. by NFS or NIS). This may reportedly lead to disruption of network services, disclosure of sensitive information, or potentially compromise of other systems.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57766-1

- **CVS Buffer Overflow and Denial of Service Vulnerabilities**

"Denial of Service"

Multiple vulnerabilities have been reported in CVS, where one has an unknown impact and others which potentially can be exploited by malicious people to cause a DoS (Denial of Service) and compromise a vulnerable system.

1) An unspecified boundary error can be exploited to cause a buffer overflow and potentially execute arbitrary code.

2) Some memory leaks and NULL pointer dereferences may be exploited to cause a DoS.

3) An unspecified error caused due to an arbitrary free has an unknown impact.

4) Some errors in the contributed Perl scripts can be exploited to execute arbitrary code via a malicious Perl library.

Successful exploitation requires that the user has commit access and that one of the contributed Perl scripts has been installed improperly.

References:
https://ccvs.cvshome.org/source/browse/ccvs/NEWS?rev=1.116.2.127&content-type=text/x-cvsweb-markup

- **Mozilla Firefox Multiple Vulnerabilities**

"Cross-site scripting attacks; Bypass certain security restrictions"

Multiple vulnerabilities have been reported in Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and compromise a user's system.

1) An input validation error when processing the "PLUGINSPAGE" attribute of the "EMBED" tag for non-installed plugins can be exploited to inject arbitrary JavaScript code in the "chrome" via a specially crafted "PLUGINSPAGE" attribute.

Successful exploitation may allow execution of arbitrary code, but requires that the user clicks the "Manual Install" button.

2) An error, where blocked popups opened through the GUI incorrectly runs with "chrome" privileges, can be exploited to execute arbitrary code via a specially crafted "javascript:" URI.

Successful exploitation requires that the user opens a blocked popup.

3) An error, where the global scope of a window or tab in certain situations is not properly cleaned before navigating to a new web site, can be exploited to execute arbitrary script code in a user's browser session in context of the new site.

4) An error, where the URL of a "favicons" icon for a web site is not verified before being changed via JavaScript, can be exploited to execute arbitrary script code with escalated privileges via a specially crafted "javascript:" URI.

Successful exploitation may allow execution of arbitrary code.

5) An error, where the action URL of a search plugin is not verified before being used to perform a search, can be exploited to execute arbitrary script code in a user's browser session in context of the current web site, but requires that the user is tricked into installing a search plugin with a specially crafted "javascript:" URI.

Successful exploitation may allow execution of arbitrary code, if a search is performed when the current web site runs with escalated privileges (e.g. "about:plugins" and "about:config").

6) An error in the way links are opened in the sidebar using the "_search" target can be exploited to execute arbitrary script code in a user's browser session in context of an arbitrary website via a specially crafted "javascript:" URI.

Successful exploitation may allow execution of arbitrary code.

7) Some input validation errors when handling parameters of invalid types passed to certain "InstallTrigger" and "XPInstall" related objects via JavaScript may be exploited to execute arbitrary code.

8) Some errors, where certain privileged UI code does not properly validate DOM nodes from the content window, can be exploited to execute arbitrary code.

Successful exploitation may require some user interaction.

References:
http://www.mozilla.org/security/announce/mfsa2005-34.html
http://www.mozilla.org/security/announce/mfsa2005-35.html
http://www.mozilla.org/security/announce/mfsa2005-36.html
http://www.mozilla.org/security/announce/mfsa2005-37.html
http://www.mozilla.org/security/announce/mfsa2005-38.html
http://www.mozilla.org/security/announce/mfsa2005-39.html
http://www.mozilla.org/security/announce/mfsa2005-40.html
http://www.mozilla.org/security/announce/mfsa2005-41.html
http://www.kb.cert.org/vuls/id/973309
http://www.kb.cert.org/vuls/id/519317

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