netVigilance

ScoutNews Team

May 6, 2005
Issue # 18

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

In the news; evil twins, Time-Warner is latest victim of personal information loss. It's raining Spam and hacking for cash shows no sign of letting up.

Enjoy reading

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

Top Security News Stories this Week

- **Time-Warner misplaces personal information of 600,000 current and former employees.**

Time Warner reported that a shipment of backup tapes intended for offsite storage went missing for over a month. Although there is no evidence that the persona information on the tapes has been misused; all major credit reporting agencies and the US Secret Service have been notified.

ComputerWorld

Full Story :
http://www.computerworld.com/securitytopics/security/story/0,10801,101500,00.html?from=story%5Fkc

http://money.cnn.com/2005/05/02/news/fortune500/security_timewarner/index.htm?cnn=yes

❖ Hackers getting more devious to stay ahead of security technology

At the risk of repeating myself; Phishing seems to be the method of choice for hackers that are aimed at stealing as opposed to simply causing trouble.

New types of attacks like ‘drive-by downloading’ and ‘evil twin attacks’ have emerged to circumvent advances in digital security.

Newhouse News Service

Read more here:
http://www.newhousenews.com/archive/coughlin050505.html

❖ April brings showers of Spam

The return of the SOBER virus, Russian language spam and corporate desktop targeting causes sharp increase in Spam volume for April.

Some of the new Spam attacks actually morph as the relative success of the content is measured.

Yahoo

Related Links:
http://biz.yahoo.com/iw/050505/086123.html

❖ Wireless Security Pointers

A story out of abc News affiliate in Salt Lake City, give helpful advice on securing your laptop against ‘evil twin attacks’ in wireless hot spots. Worth the read.

abc News

Full Story:
http://www.4utah.com/local_news/featured_websites/story.aspx?content_id=06668FC3-5F34-4714-B311-9EE829421E06

New Vulnerabilities Tested in SecureScout

❖ 13232 Oracle Database Server - Oracle HTTP Server (SSL) component unspecified error (apr-2005/DB22)

An unspecified error in the Oracle HTTP Server (SSL) 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

- ❖ **13233 Oracle Database Server - Oracle HTTP Server (SSL) component unspecified error (apr-2005/DB23)**

An unspecified error in the Oracle HTTP Server (SSL) 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

- ❖ **13234 Oracle Database Server - Oracle HTTP Server (SSL) component unspecified error (apr-2005/DB24)**

An unspecified error in the Oracle HTTP Server (SSL) 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

❖ 15181 Ethereal Multiple Protocol Dissector Vulnerabilities (Remote File Checking)

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

The vulnerabilities are caused due to various types of errors including NULL pointer dereference errors, format string errors, and boundary errors in a multitude of protocol dissectors.

Successful exploitation causes Ethereal to stop responding, consume a large amount of system resources, crash, or execute arbitrary code.

The vulnerabilities affect versions 0.8.14 through 0.10.10.

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

References:

Original Advisory:

http://www.ethereal.com/appnotes/enpa-sa-00019.html

Product:

http://www.ethereal.com/

Other references:

http://secunia.com/advisories/15144/

CVE Reference: CAN-2005-1281

❖ 15182 Ethereal RADIUS Protocol Dissector Vulnerabilities (Remote File Checking)

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

Boundary errors in the "dissect_a11_radius()" function in "packet-3g-a11.c" used for RADIUS authentication dissection can be exploited to cause a stack-based buffer overflow by sending a specially crafted CDMA2000 A11 packet.

This vulnerability affects versions 0.10.3 through 0.10.9.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00018.html

Product:
http://www.ethereal.com/

Other references:
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-04
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-05
http://secunia.com/advisories/14540/

CVE Reference: CAN-2005-0699, CAN-2005-0704, CAN-2005-0705, CAN-2005-0739, CAN-2005-0765, CAN-2005-0766

❖ 15183 Ethereal IAPP Protocol Dissector Vulnerabilities (Remote File Checking)

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

A boundary error in the "dissect_pdus()" function of the IAPP dissector can be exploited to cause a buffer overflow via a specially crafted packet.

This vulnerability affects versions 0.9.1 through 0.10.9.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00018.html

Product:
http://www.ethereal.com/

Other references:
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-04
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-05
http://secunia.com/advisories/14540/

CVE Reference: CAN-2005-0699, CAN-2005-0704, CAN-2005-0705, CAN-2005-0739, CAN-2005-0765, CAN-2005-0766

❖ 15184 Ethereal Etheric Protocol Dissector Vulnerabilities (Remote File Checking)

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

A boundary error in the Etheric dissector can be exploited to cause a buffer overflow via a specially crafted packet.

This vulnerability affects versions 0.10.7 through 0.10.9.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00018.html

Product:
http://www.ethereal.com/

Other references:
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-04
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-05
http://secunia.com/advisories/14540/

CVE Reference: CAN-2005-0699, CAN-2005-0704, CAN-2005-0705, CAN-2005-0739, CAN-2005-0765, CAN-2005-0766

❖ 15185 Ethereal GPRS-LLC Protocol Dissector Vulnerabilities (Remote File Checking)

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

An unspecified error in the GPRS-LLC dissector can be exploited to cause a crash when the "ignore cipher bit" option is enabled.

This vulnerability affects versions 0.10.7 through 0.10.9.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00018.html

Product:
http://www.ethereal.com/

Other references:
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-04
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-05

http://secunia.com/advisories/14540/

CVE Reference: CAN-2005-0699, CAN-2005-0704, CAN-2005-0705, CAN-2005-0739, CAN-2005-0765, CAN-2005-0766

❖ 15621 Netscape DOM Nodes Validation Vulnerability (Remote File Checking)

A new remote type vulnerability has been reported in Netscape, which can be exploited by malicious people to compromise a user's system.

This is a code execution type vulnerability.
DOM nodes are not properly validated from the content window.

Tested software versions:
Netscape 7.2
Exact user-agent in use:
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.2) Gecko/20040804 Netscape/7.2 (ax)

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

References:

Original Advisory:
http://www.networksecurity.fi/advisories/netscape-dom.html

Product HomePage:
http://channels.netscape.com/ns/browsers/default.jsp

Other references:
http://secunia.com/advisories/15135/
http://www.mozilla.org/security/announce/mfsa2005-41.html
https://bugzilla.mozilla.org/show_bug.cgi?id=289083

CVE Reference: CAN-2005-1160

❖ 15622 Netscape GIF Image Netscape Extension 2 Buffer Overflow (Remote File Checking)

A vulnerability has been reported in Netscape, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability has been confirmed in version 7.2 and has also been reported in version 6.2.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.networksecurity.fi/advisories/netscape-gif.html

Product HomePage:
http://channels.netscape.com/ns/browsers/default.jsp

Other references:
http://secunia.com/advisories/15103/
http://www.mozilla.org/security/announce/mfsa2005-30.html
https://bugzilla.mozilla.org/show_bug.cgi?id=285595

CVE Reference: CAN-2005-0399

New Vulnerabilities found this Week

❖ **Netscape GIF Image Netscape Extension 2 Buffer Overflow**
"Code Execution"

A vulnerability has been reported in Netscape, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability has been confirmed in version 7.2 and has also been reported in version 6.2.3. Other versions may also be affected.

References:
http://www.networksecurity.fi/advisories/netscape-gif.html
http://secunia.com/advisories/14654/

❖ **Netscape DOM Nodes Validation Vulnerability**
"Code Execution"

A vulnerability has been reported in Netscape, which can be exploited by malicious people to compromise a user's system.

The vulnerability has been confirmed in version 7.2. Other versions may also be affected.

References:
http://www.networksecurity.fi/advisories/netscape-dom.html
http://secunia.com/advisories/14992/

❖ **Adobe SVG Viewer Local File Detection and libpng Vulnerability**
"Code Execution; Enumerate Files"

A vulnerability and a weakness have been reported in Adobe SVG Viewer, which can be exploited by malicious people to enumerate files on a user's system or potentially compromise it.

1) An error in the ActiveX control (NPSVG3.dll) makes it possible for malicious web pages to determine whether or not a particular file exists on a user's system by specified the particular file in the "src" property.

The weakness affects versions 3.02 and prior.

2) An error in libpng can potentially be exploited to execute arbitrary code on a user's system via a specially crafted PNG image.

The vulnerability affects version 3.01 and prior.

References:
http://www.hyperdose.com/advisories/H2005-07.txt
http://secunia.com/advisories/12219/

❖ PostgreSQL Character Conversion and tsearch2 Module Vulnerabilities

“Denial of Service”

Two vulnerabilities have been reported in PostgreSQL, which can be exploited by malicious users to cause a DoS (Denial of Service) or potentially gain escalated privileges.

1) Missing validation of arguments supplied to the functions supporting client-to-server character set conversion can be exploited by unprivileged users when calling the functions from SQL commands.

The vulnerability affects versions 7.3.* through 8.0.*.

2) The contrib/tsearch2 module misdeclares the return type of several functions, which breaks the type safety of "internal". The impact has reportedly not been investigated, but can at least crash the backend.

The vulnerability affects versions 7.4 and later with the contrib/tsearch2 module installed.

References:
http://www.postgresql.org/about/news.315

❖ Avaya Kerberos Telnet Client vulnerabilities

Avaya has issued an update for krb5. This fixes two vulnerabilities, which can be exploited by malicious people to compromise a user's system.

References:
http://support.avaya.com/elmodocs2/security/ASA-2005-088_RHSA-2005-330.pdf

http://secunia.com/advisories/14745

❖ Linux Kernel Local Denial of Service Vulnerabilities

"Denial Of Service"

Two vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

1) The it87 and via686a hardware monitoring drivers create the sysfs file "alarms" with insecure permissions granting write access to the file. This can be exploited to exhaust all available CPU resources by writing to the file.

2) An error in the "key_user_lookup()" function in "security/keys/key.c" can be exploited to crash the kernel.

References:
http://kernel.org/

❖ BIG-IP / 3-DNS ICMP Handling Denial of Service Vulnerability

"Denial Of Service"

F5 Networks has acknowledged a vulnerability in BIG-IP and 3-DNS, which can be exploited by malicious people to cause a DoS (Denial of Service).

NOTE: Only the management interface on BIG-IP Local Traffic Manager is affected and not the device itself.

References:
http://tech.f5.com/home/bigip/solutions/advisories/sol4583.html
http://tech.f5.com/home/bigip-next/solutions/advisories/sol4584.html

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.

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