netVigilance

ScoutNews Team **March 11, 2005**
Issue # 10

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Could a Hacker or Cyber-terrorist bring down the N. American power grid? Hackers find short path to consumer records, you could be an unwilling assistant is a hacker slang war and get those NT4 systems upgraded!

Read on and stay safe 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

- **Nations power supply at risk from Hacker attack.**

Cyber Security at the nation's electric companies is spotty and not standardized; leaving the North American power grid vulnerable to a cyber-attack. Security of the U.S. power supply is only as good as the security of the weakest electric company.

Patrick H. Wood III, the chairman of the Federal Energy Regulatory Commission (news - web sites), warned top electric company officials in a private meeting in January that they need to focus more heavily on cyber-security

After seeing a demonstration at the Energy Department's Idaho National

Laboratory of how a skilled hacker could disrupt service and even damage power generation equipment; Woods stated: "I wished I'd had a diaper on."

Richard A. Clarke, a former counterterrorism chief in the Clinton and Bush administrations was quoted saying: "A sophisticated hacker, which is probably a group of hackers . . . could probably get into each of the three U.S. North American power [networks] and could probably bring sections of it down if they knew how to do it,"
Washington Post

Full Story:
http://story.news.yahoo.com/news?tmpl=story&cid=1804&e=2&u=/washpost/a25738_2005mar10

- **Like ChoicePoint and Bank of America; LexisNexis now hacked, 32,000 consumer records stolen.**

In an attack that is similar to it's rival ChoicePoint; LexisNexis disclosed on Wednesday that it's database security was compromised allowing access to at least 32,000 consumer records.

It appears that this trend is growing and with hacker success sans prosecution; it looks to get worse before it gets better.

Reforms must be in order; ChoicePoint is currently under investigation by the FTC and SEC and facing a class-action lawsuit from shareholders (Related story; http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,100239,00.html) .

I found that you can have your information removed from the LexisNexis database, see link:
http://www.lexisnexis.com/terms/privacy/data/removal.asp

As far as BofA and ChoicePoint I could not find information on how to get back control of my sensitive information.

Full Story:
http://story.news.yahoo.com/news?tmpl=story&cid=77&e=1&u=/mc/hackersbreachlexisnexisgrabinfoon32000people

IDG News Service

- **Windows NT web servers considered high risk.**

It is estimated the there are websites numbering in the hundreds of thousands still running Windows NT. These servers are considered extremely vulnerable to hacking since Microsoft ended support for NT4 in December of '04.

A bug existing in the MS protocol; Server Message Block (SMB), is to be considered High Risk. The hole was patched for current MS OS versions a month ago, but NT4 systems are running unprotected.

TechWeb News

Full Story:
http://www.informationweek.com/story/showArticle.jhtml;jsessionid=U4122ZGCB25XMQSNDBCCKHSCJUMEKJVN?articleID=159400893&tid=6004

- **Cyber punks exploit MSN vulnerabilities to launch slang-war.**

In the 'Too much time on their hands' category, a tale of pretzel logic from the IT underworld.

A new worm on the loose called 'Fatso' exploits MSN users to perpetrate a slang war against author of Assiral.A worm. Fatso sends an instant message with a URL that, when clicked, causes the PC to download the virus that broadcasts a taunt to Assiral.A writer; 'LARISSA'. Assiral.A was written and propagated to remove the Bropia worm, but Assirial.A is not harmless either.

Maybe, you say; it's great that these hackers are spending their idle hours engaging in 'spitting contests' against each other, unfortunately they are using

your MSN client to do so.

Related Links:

http://www.ebcvg.com/news.php?id=4732

http://www.andpop.com/article/4014

New Vulnerabilities Tested in SecureScout

- **14702 Sun Java Runtime Environment Java Plug-in JavaScript Security Restriction Bypass Vulnerability (Remote File Checking)**

A vulnerability is reported to exist in the access controls of the Java to JavaScript data exchange within web browsers that employ the Sun Java Plug-in. Reports indicate that it is possible for a malicious website that contains JavaScript code to exploit this vulnerability to load a dangerous Java class and to pass this class to an invoked applet.

This issue has been fixed in J2SE v 1.4.2_06.

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

References:

Original Advisory:
http://securityfocus.com/archive/1/382072
http://securityfocus.com/archive/1/382281
http://securityfocus.com/archive/1/381940

Other References:
http://securityfocus.com/bid/11726
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57741-1

Product HomePage:
http://java.sun.com/j2se/

CVE Reference: CAN-2004-1029

- **15169 Ethereal "dissect_a11_radius()" Buffer Overflow Vulnerability (Remote File Checking)**

Leon Juranic has reported a vulnerability in Ethereal, which potentially can be exploited by malicious people to compromise a vulnerable system.

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

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 0.10.9 and prior versions including the 3G-A11 dissector.

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

References:

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

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

CVE Reference: none.

- **15170 Ethereal COPS Packet Dissector Vulnerabilities (Remote File Checking)**

An unspecified error in the COPS dissector can be exploited to cause the process to enter an infinite loop and consume available CPU resources.

The vulnerability affects versions 0.10.6 through 0.10.8.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00017.html

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

Other references:
http://secunia.com/advisories/13946/

CVE Reference: CAN-2005-0006 CAN-2005-0007 CAN-2005-0008 CAN-2005-0009 CAN-2005-0010 CAN-2005-0084

❖ 15171 Ethereal DLSw Packet Dissector Vulnerabilities (Remote File Checking)

An unspecified error in the DLSw dissector can be exploited to crash the process.

The vulnerability affects versions 0.10.6 through 0.10.8.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00017.html

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

Other references:
http://secunia.com/advisories/13946/

CVE Reference: CAN-2005-0006 CAN-2005-0007 CAN-2005-0008 CAN-2005-0009 CAN-2005-0010 CAN-2005-0084

❖ 15172 Ethereal DNP Packet Dissector Vulnerabilities (Remote File Checking)

An unspecified error in the DNP dissector can be exploited to corrupt memory content.

The vulnerability affects versions 0.10.5 through 0.10.8.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00017.html

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

Other references:
http://secunia.com/advisories/13946/

CVE Reference: CAN-2005-0006 CAN-2005-0007 CAN-2005-0008 CAN-2005-0009 CAN-2005-0010 CAN-2005-0084

- **15173 Ethereal Gnutella Packet Dissector Vulnerabilities (Remote File Checking)**

An unspecified error in the Gnutella dissector can be exploited to crash the process.

The vulnerability affects versions 0.10.6 through 0.10.8.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00017.html

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

Other references:
http://secunia.com/advisories/13946/

CVE Reference: CAN-2005-0006 CAN-2005-0007 CAN-2005-0008 CAN-2005-0009 CAN-2005-0010 CAN-2005-0084

- **15174 Ethereal MMSE Packet Dissector Vulnerabilities (Remote File Checking)**

An unspecified error in the MMSE dissector may cause it to free static memory.

The vulnerability affects versions 0.10.4 through 0.10.8.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00017.html

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

Other references:
http://secunia.com/advisories/13946/

CVE Reference: CAN-2005-0006 CAN-2005-0007 CAN-2005-0008 CAN-2005-0009 CAN-2005-0010 CAN-2005-0084

- **15175 Ethereal X11 Packet Dissector Vulnerabilities (Remote File Checking)**

A boundary error in the X11 dissector can be exploited to cause a buffer overflow and potentially execute arbitrary code.

The vulnerability affects versions 0.8.10 through 0.10.8.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00017.html

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

Other references:
http://secunia.com/advisories/13946/

CVE Reference: CAN-2005-0006 CAN-2005-0007 CAN-2005-0008 CAN-2005-0009 CAN-2005-0010 CAN-2005-0084

- **15288 Trillian Basic PNG Image Buffer Overflow Vulnerability (Remote File Checking)**

Tal zeltzer has reported a vulnerability in Trillian Basic, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the processing of PNG images. This can be exploited to cause a buffer overflow by sending a specially crafted display image to a vulnerable client via e.g. the MSN protocol.

Successful exploitation can lead to execution of arbitrary code.

The vulnerability has been reported in version 3.0. Other versions may also be affected.

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

References:
http://www.trillian.cc/
http://www.securityfocus.com/bid/11142
http://secunia.com/advisories/14470/
http://www.securiteam.com/exploits/5KP030KF5E.html

CVE Reference: none.

- **16013 ArGoSoft FTP Server "DELE" Buffer Overflow Vulnerability (FTP)**

ArGoSoft FTP Server is an FTP server for Windows 95/98/NT.

CorryL has discovered a vulnerability in ArGoSoft FTP Server, which can be exploited by malicious users to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the handling of the "DELE" command. This can be exploited to cause a buffer overflow by supplying an overly long argument to the "DELE" command (more than 2000 characters).

Successful exploitation allows execution of arbitrary code, but requires that a user has permissions to delete files.

The vulnerability has been confirmed in version 1.4.2.8. Other versions may also be affected.

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

References:
http://secunia.com/advisories/14526/
http://www.argosoft.com/applications/ftpserver/

CVE Reference: none.

New Vulnerabilities found this Week

- **HP Tru64 Message Queue Denial of Service Vulnerability**

"Denial of Service"

A vulnerability has been reported in HP Tru64 UNIX, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in the systems message queue and impacts multiple processes.

The following supported versions are affected:
* HP Tru64 Unix V5.1B-2/PK4
* HP Tru64 Unix V5.1B-1/PK3
* HP Tru64 Unix V5.1A PK6
* HP Tru64 Unix V4.0G PK4
* HP Tru64 Unix V4.0F PK8

References:

http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01109

- **Ethereal "dissect_a11_radius()" Buffer Overflow Vulnerability**

"Stack-based buffer overflow, execution of arbitrary code"

A vulnerability has been reported in Ethereal, which potentially can be exploited by malicious people to compromise a vulnerable system.

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

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 0.10.9 and prior versions including the 3G-A11 dissector.

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

- **Trillian Basic PNG Image Buffer Overflow Vulnerability**

"Buffer overflow, execution of arbitrary code"

Tal zeltzer has reported a vulnerability in Trillian Basic, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the processing of PNG images. This can be exploited to cause a buffer overflow by sending a specially crafted display image to a vulnerable client via e.g. the MSN protocol.

Successful exploitation can lead to execution of arbitrary code.

The vulnerability has been reported in version 3.0. Other versions may also be affected.

- **grsecurity Unspecified RBAC System Privilege Escalation**

"Gain escalated privileges"

A vulnerability has been reported in grsecurity, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unspecified error in the RBAC (Role-Based Access Control) system, which effectively gives every subject the "O" flag. This can e.g. be exploited via LD_PRELOAD or ptrace by root users to gain the privileges of any other process.

Successful exploitation requires use of the RBAC system.

References:
http://www.grsecurity.org/news.php#grsec213

- **PaX Unspecified Privilege Escalation Vulnerability**

"Gain escalated privileges"

A vulnerability has been reported in PaX, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unspecified error related to the VMA mirroring functionality and allows execution of arbitrary code with escalated privileges.

Successful exploitation requires that the SEGMEXEC or RANDEXEC feature is enabled.

The vulnerability affects all releases since September 2003.

References:
http://pax.grsecurity.net/

- **Xerox MicroServer Web Server Unauthorised Access Vulnerability**

"Bypass certain security restrictions"

A vulnerability has been reported in Xerox MicroServer Web Server, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an unspecified error making it possible to gain unauthorized access to the device.

Successful exploitation allows manipulation of the system configuration.

The vulnerability affects the following products:
* WorkCentre M35/M45/M55 (versions 2.028.11.000 through 2.97.20.032 and versions 4.84.16.000 through 4.97.20.032)
* WorkCentre M165/M175 (versions 6.47.30.000 through 6.47.33.008 and versions 8.47.30.000 through 8.47.33.008)
* WorkCentre Pro 35/45/55 (versions 3.028.11.000 through 3.97.20.032)
* WorkCentre Pro 65/75/90 (versions 1.001.00.060 through 1.001.02.084)
* WorkCentre Pro 32/40 Color (versions 0.001.00.060 through 0.001.02.081)
* WorkCentre Pro 165/175 (versions 7.47.30.000 through 7.47.33.008)
* WorkCentre Pro Color 2128/2636/3545 (version 0.001.04.044)

References:
http://www.xerox.com/downloads/usa/en/c/cert_XRX05_005.pdf

❖ **X11 libXpm XPM Image Buffer Overflow Vulnerability**

"Buffer overflow, execution of arbitrary code"

Chris Gilbert has reported a vulnerability in libXpm, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to boundary errors in "GetImagePixels()" and "PutImagePixels()". This may be exploited to cause a buffer overflow when a specially crafted XPM image file is processed.

Successful exploitation may potentially allow execution of arbitrary code.

References:
http://www.gentoo.org/security/en/glsa/glsa-200503-08.xml

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