netVigilance

ScoutNews Team **April 8, 2005**
Issue # 14

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review
Top Security News Stories this Week
New Test Cases Tested in SecureScout
New Vulnerabilities this Week

This Week in Review

Honestly, I'm not a gloomy guy, this

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

- **Phishing attacks getting ever more insidious and damaging**

How cheerfully he seems to grin, How neatly spreads his claws, And welcomes little fishes in With gently smiling jaws! *– Lewis Carroll; Alice's Adventures in Wonderland*

Phishing, the most popular method of identity theft; seems to know no bounds. Three Phishing attacks of note this week target unsuspecting users, stealing passwords, contacts and credit card numbers.

In one attack, users receive a messge "You have just received a virtual postcard from a family member!". This bogus link in the message launches a Trojan to hijack the mIRC; a mechanism used for chat services, to steal your passwords.

Another scam involves several bogus websites offering cheap airfare. The website asks

for personal information including credit card info. The site then tells the user that an error has occurred in processing and gives other payment instructions, just to keep up assurances.

Phishing attacks are growing at a rate of about 26% per month and the sophistication is increasing at a pace that stays well ahead of anti-virus software capabilities. Always consider the source (from line) of all email messages, when in doubt, throw it out.

TechWeb / Cnet

Related Links :

Virtual postcard scam :
http://www.techweb.com/wire/security/160501543
Bogus Airfare sites :
http://www.techweb.com/wire/security/160502372
Phishing forecast :
http://asia.cnet.com/news/security/0,39037064,39224951,00.htm

- **Europeans increasingly wary of online transactions**

A recent Forrester research study, 30% of the 23,000 person study group says that they have confidence in the security of their personal information. Lack of confidence in online transactions is not only slowing the rate at which new customers are joining, but also causing existing online banking customers to defect. For 2002, 3 Million existing online banking customers quit and 1 Million in the UK exited.

COMPUTERWORLD

Full Story:
http://www.computerworld.com/printthis/2005/0,4814,100736,00.html

- **Business impact of Virus attacks getting worse**

Reported virus infections by Business rose 50% in 2004 according to ICSA Labs division of Cybertrust. The survey also indicates that downtime is compounded with each new threat encountered.

Prevention is the best medicine; frequent Vulnerability Assessments and up-to-date anti-virus is key to preventing infection.

InformationWeek

Related Link:
http://www.informationweek.com/story/showArticle.jhtml?articleID=160501452

New Vulnerabilities Tested in SecureScout

- **15180 Adobe Reader / Adobe Acrobat Local Files Detection and Denial of Service (Remote File Checking)**

Two weaknesses have been reported in Adobe Reader and Adobe Acrobat, which can be exploited by malicious people to enumerate files on a user's system or crash the application.

1) An error in the "LoadFile()" method makes it possible to determine if a queried local file exists via e.g. a malicious web site invoking the Internet Explorer ActiveX control directly.

2) An error within the processing of certain PDF documents can be exploited to crash the application via a PDF document containing a negative root page node "Count" value.

The weaknesses have been reported in versions 7.0 and prior for Windows.

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

References:

Original advisories:
http://www.adobe.com/support/techdocs/331465.html
http://www.adobe.com/support/techdocs/331468.html

Other references:
http://secunia.com/advisories/14813/

CVE Reference: CAN-2005-0035 CAN-2005-0492

- **15583 Cisco VPN Concentrator 3000 Series HTTPS Packet Denial of Service (CSCeg11424)**

The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

A malicious user may be able to send a crafted attack via SSL (Secure Sockets Layer) to the concentrators which may cause the device to reload, and/or drop user connections.

Repeated exploitation will create a sustained DoS (denial of service).

The vulnerability affects devices running software version 4.1.7.A and prior.

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

References:

* Cisco Security Advisory: Cisco VPN 3000 Concentrator Vulnerable to Crafted SSL Attack (CSCeg11424):
http://www.cisco.com/warp/public/707/cisco-sa-20050330-vpn3k.shtml

Other references:
http://secunia.com/advisories/14784/

CVE Reference: None.

❖ **15591 Cisco IOS IKE XAUTH Implementation Security Bypass Vulnerabilities (CSCin82407/CSCeg00277)**

Two vulnerabilities have been reported in Cisco IOS, which can be exploited by malicious people to bypass certain security restrictions.

1) An error in the processing of IKE (Internet Key Exchange) XAUTH messages can be be exploited via specially crafted packets to complete authentication and gain access to network resources.

Successful exploitation requires knowledge of the shared group key to complete the IKE Phase 1 negotiation.

2) An error within the handling of ISAKMP profile attributes may cause the attributes to not be processed and result in a deadlock condition, which can be exploited to establish an unauthorised IPsec SA (Security Association).

This vulnerability only affects ISAKMP profiles matched by certificate maps.

The vulnerabilities affect network devices running the Cisco IOS 12.2T, 12.3, and 12.3T release trains and are configured for Cisco Easy VPN Server XAUTH version 6 authentication.

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

References:

* Cisco Security Advisory: Vulnerabilities in the Internet Key Exchange Xauth Implementation (CSCin82407/CSCeg00277):
http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml

Other references:

http://secunia.com/advisories/14853/

CVE Reference: None.

❖ **15592 Cisco IOS Secure Shell Server Denial of Service Vulnerabilities (CSCed65778/CSCed65285)**

Two vulnerabilities have been reported in Cisco IOS, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) An error when acting as a SSH v2 server for remote management and authenticating against a TACACS+ server can be exploited to cause a vulnerable device to reload.

2) A memory leak can be exploited to exhaust memory resources when authenticating SSH users against a TACACS+ server and login fails due to invalid credentials.

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

References:

* Cisco Security Advisory: Vulnerabilities in Cisco IOS Secure Shell Server (CSCed65778/CSCed65285):
http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml

Other references:
http://secunia.com/advisories/14854/

CVE Reference: None.

❖ **15593 Mozilla Firefox JavaScript Engine Information Disclosure Vulnerability (Remote File Checking)**

A vulnerability has been discovered in Mozilla Firefox, which can be exploited by malicious people to gain knowledge of potentially sensitive information.

The vulnerability is caused due to an error in the JavaScript engine, as a "lambda" replace exposes arbitrary amounts of heap memory after the end of a JavaScript string.

Successful exploitation may disclose sensitive information in memory.

The vulnerability has been confirmed in versions 1.0.1 and 1.0.2. Other versions may

also be affected.

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

References:

Original Advisory:
http://cubic.xfo.org.ru/index.cgi?read=53004
https://bugzilla.mozilla.org/show_bug.cgi?id=288688

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

Other references:
http://secunia.com/advisories/14820/

CVE Reference: None.

❖ **15594 Mozilla JavaScript Engine Information Disclosure Vulnerability (Remote File Checking)**

A vulnerability has been discovered in Mozilla, which can be exploited by malicious people to gain knowledge of potentially sensitive information.

The vulnerability is caused due to an error in the JavaScript engine, as a "lambda" replace exposes arbitrary amounts of heap memory after the end of a JavaScript string.

Successful exploitation may disclose sensitive information in memory.

The vulnerability has been confirmed in version 1.7.6. Other versions may also be affected.

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

References:

Original Advisory:
http://cubic.xfo.org.ru/index.cgi?read=53004
https://bugzilla.mozilla.org/show_bug.cgi?id=288688

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

Other references:
http://secunia.com/advisories/14821/

CVE Reference: None.

❖ **15595 Netscape JavaScript Engine Information Disclosure Vulnerability (Remote File Checking)**

A vulnerability has been discovered in Netscape, which can be exploited by malicious people to gain knowledge of potentially sensitive information.

The vulnerability is caused due to an error in the JavaScript engine, as a "lambda" replace exposes arbitrary amounts of heap memory after the end of a JavaScript string.

Successful exploitation may disclose sensitive information in memory.

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

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

References:

Original Advisory:
http://cubic.xfo.org.ru/index.cgi?read=53004
https://bugzilla.mozilla.org/show_bug.cgi?id=288688

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

Other references:
http://secunia.com/advisories/14804/

CVE Reference: None.

❖ **18112 MailEnable SMTP DNS Lookup Denial of Service Vulnerability**

A vulnerability has been reported in MailEnable, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error when processing DNS responses. This can be exploited to crash the SMTP service by returning a DNS response containing over 100 MX records.

MailEnable Standard 1.71 fixes the issue.

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

References:

Original advisory:
http://www.mailenable.com/hotfix/

Other references:
http://secunia.com/advisories/12493/

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

CVE Reference: GENERIC-MAP-NOMATCH

❖ 18113 MailEnable Standard SMTP Format String Vulnerability

Mati Aharoni has discovered a vulnerability in MailEnable Standard, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

The vulnerability is caused due to a format string error in the handling of command arguments in the SMTP communication. This can be exploited to crash a vulnerable service or potentially execute arbitrary code by supplying a specially crafted command argument.

The vulnerability has been confirmed in version 1.8. Other versions may also be affected.

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/393566

Other references:
http://secunia.com/advisories/14627
http://marc.theaimsgroup.com/?l=bugtraq&m=111108519331738&w=2

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

CVE Reference: CAN-2005-0804

❖ 18114 MailEnable "EHLO" command Denial of Service Vulnerability

An error in the handling of the "EHLO" command in the SMTP service can be exploited to crash a vulnerable service by supplying an overly long argument in unicode.

The vulnerabilities have been reported in MailEnable Enterprise version 1.04, and in MailEnable Professional version 1.54 and prior.

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

References:

Original advisory:
http://secunia.com/advisories/14812/

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

CVE Reference: CAN-2005-0804

New Vulnerabilities found this Week

- **Linksys WET11 Password Change Security Bypass Vulnerability**

  "bypass certain security restrictions"

  Kristian Hermansen has reported a vulnerability in Linksys WET11, which can be exploited by malicious people to bypass certain security restrictions.

  The vulnerability is caused due to an error where the device password can be changed without providing the old password. This can be exploited to set a blank password and gain access to the device.

  NOTE: In version 1.5.4, successful exploitation requires that a user has logged in recently.

  The vulnerability has been reported in version 1.5.4. Other versions may also be affected.

  References:
  http://secunia.com/advisories/14871/

- **MailEnable IMAP "LOGIN" Command Buffer Overflow Vulnerability**

  "Denial of Service"

  H D Moore has discovered a vulnerability in MailEnable, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

  The vulnerability is caused due to a boundary error in the IMAP service when handling the "LOGIN" command. This can be exploited to cause a buffer overflow by supplying an overly long argument (more than 1024 bytes).

  Successful exploitation may allow execution of arbitrary code.

The vulnerability has been confirmed in MailEnable Professional version 1.54 with hotfix MEIMSM-HF050404 applied. Other versions may also be affected.

References:
http://secunia.com/advisories/14870/

- **Cisco IOS Secure Shell Server Denial of Service Vulnerabilities**

"Denial of Service"

Two vulnerabilities have been reported in Cisco IOS, which can be exploited by malicious people to cause a DoS (Denial of Service).

1) An error when acting as a SSH v2 server for remote management and authenticating against a TACACS+ server can be exploited to cause a vulnerable device to reload.

2) A memory leak can be exploited to exhaust memory resources when authenticating SSH users against a TACACS+ server and login fails due to invalid credentials.
References:
http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml

- **Cisco IOS IKE XAUTH Implementation Security Bypass Vulnerabilities**

"bypass certain security restrictions"

Two vulnerabilities have been reported in Cisco IOS, which can be exploited by malicious people to bypass certain security restrictions.

1) An error in the processing of IKE (Internet Key Exchange) XAUTH messages can be be exploited via specially crafted packets to complete authentication and gain access to network resources.

Successful exploitation requires knowledge of the shared group key to complete the IKE Phase 1 negotiation.

2) An error within the handling of ISAKMP profile attributes may cause the attributes to not be processed and result in a deadlock condition, which can be exploited to establish an unauthorised IPsec SA (Security Association).

This vulnerability only affects ISAKMP profiles matched by certificate maps.

The vulnerabilities affect network devices running the Cisco IOS 12.2T, 12.3, and 12.3T release trains and are configured for Cisco Easy VPN Server XAUTH version 6 authentication.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml

❖ **HP OpenView Network Node Manager Unspecified Denial of Service**
"Denial of Service"

A vulnerability has been reported in OpenView Network Node Manager (OV NNM), which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error.

References:
http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMA01125

❖ **Lotus Domino Web Service Denial of Service Vulnerability**
"Denial of Service"

A vulnerability has been reported in Lotus Domino, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the "NLSCCSTR.DLL" module when processing certain HTTP requests for the "cgi-bin/" directory. This can be exploited to cause a stack overflow via a specially crafted HTTP GET request containing a long string of certain UNICODE characters.

Successful exploitation may crash the "nHTTP.exe" process.

The vulnerability has been reported in versions 6.5.1 and 6.0.3. Other versions may also be affected. However, the vendor reports that the vulnerability could not be reproduced on any systems.

References:
http://www-1.ibm.com/support/docview.wss?uid=swg21202446
http://www.idefense.com/application/poi/display?id=224&type=vulnerabilities

❖ **DameWare NT Utilities / Mini Remote Control Privilege Escalation**
"gain escalated privileges"

A vulnerability has been reported in DameWare NT Utilities and DameWare Mini Remote Control, which can be exploited by malicious users to gain escalated privileges.

No further details are currently available.

The vulnerability affects:
* DameWare NT Utilities version 4.8 and prior.
* DameWare Mini Remote Control version 4.8 and prior.

References:

http://www.dameware.com/support/security/bulletin.asp?ID=SB5

- **Windows Server 2003 Local Denial of Service Vulnerabilities**

"Denial of Service"

Two vulnerabilities have been reported in Microsoft Windows Server 2003, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

1) The vulnerability is caused due to an error when the SMB redirector receives a browser announcement frame and subsequently tries to run code that is paged out. This can be exploited to cause the system to crash by e.g. retrieving a large file from a network share when the system is under heavy load.

2) The vulnerability is caused due to an error where the printer driver under certain circumstances passes an invalid color adjustment object to Windows Server 2003. This can be exploited to cause the system to crash by a user through a terminal service session, where the user opens a Microsoft Word message in Microsoft Outlook and then prints the message to a network printer.

References:
http://support.microsoft.com/kb/824721/
http://support.microsoft.com/kb/890554/
http://support.microsoft.com/kb/829422/

- **Mozilla Firefox JavaScript Engine Information Disclosure Vulnerability**

"gain knowledge of potentially sensitive information"

A vulnerability has been discovered in Mozilla Firefox, which can be exploited by malicious people to gain knowledge of potentially sensitive information.

The vulnerability is caused due to an error in the JavaScript engine, as a "lambda" replace exposes arbitrary amounts of heap memory after the end of a JavaScript string.

Successful exploitation may disclose sensitive information in memory.

The vulnerability has been confirmed in versions 1.0.1 and 1.0.2. Other versions may also be affected.

References:
https://bugzilla.mozilla.org/show_bug.cgi?id=288688
http://cubic.xfo.org.ru/index.cgi?read=53004

- **Adobe Reader / Adobe Acrobat Local Files Detection and Denial of Service**

"enumerate files on a user's system or crash the application"

Two weaknesses have been reported in Adobe Reader and Adobe Acrobat,

which can be exploited by malicious people to enumerate files on a user's system or crash the application.

1) An error in the "LoadFile()" method makes it possible to determine if a queried local file exists via e.g. a malicious web site invoking the Internet Explorer ActiveX control directly.

2) An error within the processing of certain PDF documents can be exploited to crash the application via a PDF document containing a negative root page node "Count" value.

The weaknesses have been reported in versions 7.0 and prior for Windows.

References:
http://www.adobe.com/support/techdocs/331465.html
http://www.adobe.com/support/techdocs/331468.html

- **Linux Kernel "is_hugepage_only_range()" Denial of Service**

"Denial of Service"

Daniel McNeil has reported a vulnerability in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the AIO (Asynchronous I/O) support within the "is_hugepage_only_range()" function. This can be exploited via a specially crafted program calling the "io_queue_init()" function and then exiting without calling the "io_queue_release()" function.

Successful exploitation crashes the system on PPC64 and IA64 architectures, but requires that CONFIG_HUGETLB_PAGE is enabled.

The vulnerability has been reported in versions 2.6.8 and 2.6.11. Other versions may also be affected.

References:
http://secunia.com/advisories/14718/

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