netVigilance

ScoutNews Team

September 9, 2005
Issue # 36

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Forrester analyst boils-down network security, Trojan morality police spotted, Spyware is bad (!?!) and men may need more rugged computers.

Enjoy reading

Top Security News Stories this Week

- **Matthew Friedman outlines top 4 security dangers**

Forrester Research analyst Paul Stamp purports that 4 major factors commonly lead to a weak network security posture: Social Engineering, process errors, technical vulnerabilities and inside abuse.

Networking pipeline

Full Story:

http://www.networkingpipeline.com/170700570

- **New Trojan blocks objectionable web sites and quotes Quran**

A Trojan discovered this week called Cager.A or Yusufali.A, monitors a user's IE title bar for terms that the originator deems offensive then closes down the browser and displays an English translation of a Quran verse.

Although a very low level threat, the nature of the actions of the Trojan has raised publicity.

About.com

Related Links:
http://antivirus.about.com/b/a/200124.htm

❖ Israeli security specialists claim 15% of spyware is malicious

Aladdin Knowledge Systems recently completed a study of prevalent spyware programs and found that 15% are used for criminal activity.

Websites as opposed to email messages are becoming more popular vehicles to spread Trojans and malware as public awareness increases toward the threat of Spam and unknown sources. The study also found an increase in the number of spyware applications that steal a user's information and mail it to a third party.

Source

Related Links:
http://www.redherring.com/Article.aspx?a=13405&hed=Spyware+Linked+to+Crime&sector=Industries&subsector=SecurityAndDefense

❖ Men more likely to throw things or swear in the face of computer problems

In a recent survey, Symantec polled 1,250 Canadian adults to gauge their stress levels and greatest issues around PCs and online security.

The study found that women are less likely to ask for help when encountering computer problems while Canadian men were twice as likely to "throw things" or swear when dealing with computer problems.

Not sure what all of this means yet – *Ed.*

Toronto Business Times

Full Story:
http://www.insidetoronto.ca/to/tbt/story/3021434p-3503474c.html

New Vulnerabilities Tested in SecureScout

❖ 13279 CVS execution of arbitrary code

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

CVS has been found vulnerable to an issue allowing anonymous users to execute arbitrary code.

Directory requests are not handled correctly, if a user sends a malformed directory name, it is possible to make the function return at an address that has already been freed, this allows the attacker do cause a double-free, by exploiting this through the use of other CVS commands it is possible to execute arbitrary code.

Version 1.11.4 and below are vulnerable.

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

References:

Original advisory:
http://secunia.com/advisories/7909/

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: None

❖ 13280 CVS Creation of Arbitrary Directories

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

A vulnerability has been identified in CVS, allowing malicious users to create arbitrary folders and possibly files in the root of the host's file system.

The problem is that CVS fails to detect attempts to create directories and files.

The vulnerability affects versions 1.11.9 and prior.

NOTE: Such attacks are usually not possible due to the file permissions set on host systems.

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

References:

Original advisory:
http://ccvs.cvshome.org/servlets/NewsItemView?newsID=84&JServSessionIdservlets=8u3x1myav1

Other references:
#
CONFIRM:http://ccvs.cvshome.org/servlets/NewsItemView?newsID=84&JServSessionId

servlets=8u3x1myav1

# MANDRAKE:MDKSA-2003:112
# URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2003:112

# REDHAT:RHSA-2004:003
# URL:http://www.redhat.com/support/errata/RHSA-2004-003.html

# REDHAT:RHSA-2004:004
# URL:http://www.redhat.com/support/errata/RHSA-2004-004.html

# DEBIAN:DSA-422
# URL:http://www.debian.org/security/2004/dsa-422

# CONECTIVA:CLA-2004:808
# URL:http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000808

# SGI:20040103-01-U
# URL:ftp://patches.sgi.com/support/free/security/advisories/20040103-01-U.asc

# BUGTRAQ:20031217 [OpenPKG-SA-2003.052] OpenPKG Security Advisory (cvs)
# URL:http://marc.theaimsgroup.com/?l=bugtraq&m=107168035515554&w=2

# BUGTRAQ:20040129 [FLSA-2004:1207] Updated cvs resolves security vulnerability
# URL:http://marc.theaimsgroup.com/?l=bugtraq&m=107540163908129&w=2

# XF:cvs-module-file-manipulation(13929)
# URL:http://xforce.iss.net/xforce/xfdb/13929

# OVAL:OVAL855
# URL:http://oval.mitre.org/oval/definitions/data/oval855.html

# OVAL:OVAL866
# URL:http://oval.mitre.org/oval/definitions/data/oval866.html

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2003-0977

❖ 13281 CVS boundary error in the CVS client during processing of version and author information

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

A boundary error in the CVS client during processing of version and author information can be exploited to cause a buffer overflow and execute arbitrary code by tricking a user into connecting to a malicious CVS server.

Issue has been fixed in version 1.11.20.

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

References:

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

Other references:
# DEBIAN:DSA-742
# URL:http://www.debian.org/security/2005/dsa-742

# GENTOO:GLSA-200504-16
# URL:http://www.gentoo.org/security/en/glsa/glsa-200504-16.xml

# REDHAT:RHSA-2005:387
# URL:http://www.redhat.com/support/errata/RHSA-2005-387.html

# SUSE:SuSE-SA:2005:024
# URL:http://www.novell.com/linux/security/advisories/2005_24_cvs.html

# MISC:http://bugs.gentoo.org/attachment.cgi?id=54352&action=view

# SECUNIA:14976
# URL:http://secunia.com/advisories/14976/

# XF:cvs-bo(20148)
# URL:http://xforce.iss.net/xforce/xfdb/20148

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2005-0753

❖ 13282 CVS memory leaks and NULL pointer dereferences Vulnerabilities

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

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

Issue has been fixed in version 1.11.20.

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

References:

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

Other references:
# DEBIAN:DSA-742
# URL:http://www.debian.org/security/2005/dsa-742

# GENTOO:GLSA-200504-16
# URL:http://www.gentoo.org/security/en/glsa/glsa-200504-16.xml

# REDHAT:RHSA-2005:387
# URL:http://www.redhat.com/support/errata/RHSA-2005-387.html

# SUSE:SuSE-SA:2005:024
# URL:http://www.novell.com/linux/security/advisories/2005_24_cvs.html

# MISC:http://bugs.gentoo.org/attachment.cgi?id=54352&action=view

# SECUNIA:14976
# URL:http://secunia.com/advisories/14976/

# XF:cvs-bo(20148)
# URL:http://xforce.iss.net/xforce/xfdb/20148

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2005-0753

❖ 13283 CVS arbitrary free Vulnerability

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

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

Issue has been fixed in version 1.11.20.

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

References:

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

Other references:
# DEBIAN:DSA-742
# URL:http://www.debian.org/security/2005/dsa-742

# GENTOO:GLSA-200504-16
# URL:http://www.gentoo.org/security/en/glsa/glsa-200504-16.xml

# REDHAT:RHSA-2005:387
# URL:http://www.redhat.com/support/errata/RHSA-2005-387.html

# SUSE:SuSE-SA:2005:024
# URL:http://www.novell.com/linux/security/advisories/2005_24_cvs.html

# MISC:http://bugs.gentoo.org/attachment.cgi?id=54352&action=view

# SECUNIA:14976
# URL:http://secunia.com/advisories/14976/

# XF:cvs-bo(20148)
# URL:http://xforce.iss.net/xforce/xfdb/20148

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2005-0753

❖ 13284 CVS contributed Perl scripts Vulnerabilities

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

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

Issue has been fixed in version 1.11.20.

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

References:

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

Other references:
# DEBIAN:DSA-742
# URL:http://www.debian.org/security/2005/dsa-742

# GENTOO:GLSA-200504-16
# URL:http://www.gentoo.org/security/en/glsa/glsa-200504-16.xml

# REDHAT:RHSA-2005:387
# URL:http://www.redhat.com/support/errata/RHSA-2005-387.html

# SUSE:SuSE-SA:2005:024
# URL:http://www.novell.com/linux/security/advisories/2005_24_cvs.html

# MISC:http://bugs.gentoo.org/attachment.cgi?id=54352&action=view

# SECUNIA:14976
# URL:http://secunia.com/advisories/14976/

# XF:cvs-bo(20148)
# URL:http://xforce.iss.net/xforce/xfdb/20148

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2005-0753

❖ 13285 CVS RCS diff files creation with absolute paths Vulnerability

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

A vulnerability has been discovered in CVS. It can be exploited by malicious servers to compromise clients and by malicious users to retrieve arbitrary files from a vulnerable server.

Missing validation of paths within CVS clients makes it possible to create RCS diff files with absolute paths. This may allow creation or overwriting of files in arbitrary locations on a user's system.

Successful exploitation requires that a user is tricked into connecting to a malicious CVS server.

Issue has been fixed in version 1.11.20.

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

References:

# DEBIAN:DSA-486
# URL:http://www.debian.org/security/2004/dsa-486

# FEDORA:FEDORA-2004-1620
# URL:http://marc.theaimsgroup.com/?l=bugtraq&m=108636445031613&w=2

# FREEBSD:FreeBSD-SA-04:07
# URL:ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:07.cvs.asc

# GENTOO:GLSA-200404-13
# URL:http://security.gentoo.org/glsa/glsa-200404-13.xml

# MANDRAKE:MDKSA-2004:028
# URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:028

# REDHAT:RHSA-2004:153
# URL:http://www.redhat.com/support/errata/RHSA-2004-153.html

# REDHAT:RHSA-2004:154
# URL:http://www.redhat.com/support/errata/RHSA-2004-154.html

# SGI:20040404-01-U
# URL:ftp://patches.sgi.com/support/free/security/advisories/20040404-01-U.asc

# SLACKWARE:SSA:2004-108-02
# URL:http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.400181

# SUSE:SuSE-SA:2004:008

CONFIRM:ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/002_cvs.patch

# OVAL:OVAL1042
# URL:http://oval.mitre.org/oval/definitions/data/oval1042.html

# SECUNIA:11368
# URL:http://secunia.com/advisories/11368

# SECUNIA:11371
# URL:http://secunia.com/advisories/11371

# SECUNIA:11374
# URL:http://secunia.com/advisories/11374

# SECUNIA:11375
# URL:http://secunia.com/advisories/11375

# SECUNIA:11377
# URL:http://secunia.com/advisories/11377

# SECUNIA:11380
# URL:http://secunia.com/advisories/11380

# SECUNIA:11391
# URL:http://secunia.com/advisories/11391

# SECUNIA:11400
# URL:http://secunia.com/advisories/11400

# SECUNIA:11405
# URL:http://secunia.com/advisories/11405

# SECUNIA:11548
# URL:http://secunia.com/advisories/11548

# XF:cvs-rcs-create-files(15864)
# URL:http://xforce.iss.net/xforce/xfdb/15864

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2004-0180

❖ 13286 CVS requesting content of arbitrary RCS archive files Vulnerability

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

A vulnerability has been discovered in CVS. It can be exploited by malicious servers to compromise clients and by malicious users to retrieve arbitrary files from a vulnerable server.

An error in the server makes it possible for users to request the content of arbitrary RCS archive files above $CVSROOT.

Issue has been fixed in version 1.11.15 and 1.12.7.

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

References:

# DEBIAN:DSA-486
# URL:http://www.debian.org/security/2004/dsa-486

# FEDORA:FEDORA-2004-1620
# URL:http://marc.theaimsgroup.com/?l=bugtraq&m=108636445031613&w=2

# FREEBSD:FreeBSD-SA-04:07
# URL:ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:07.cvs.asc

# GENTOO:GLSA-200404-13
# URL:http://security.gentoo.org/glsa/glsa-200404-13.xml

# MANDRAKE:MDKSA-2004:028
# URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:028

# REDHAT:RHSA-2004:153
# URL:http://www.redhat.com/support/errata/RHSA-2004-153.html

# REDHAT:RHSA-2004:154
# URL:http://www.redhat.com/support/errata/RHSA-2004-154.html

# SGI:20040404-01-U
# URL:ftp://patches.sgi.com/support/free/security/advisories/20040404-01-U.asc

# SLACKWARE:SSA:2004-108-02
# URL:http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.400181

# SUSE:SuSE-SA:2004:008

#
CONFIRM:ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/002_cvs.patch

# OVAL:OVAL1042
# URL:http://oval.mitre.org/oval/definitions/data/oval1042.html

# SECUNIA:11368
# URL:http://secunia.com/advisories/11368

# SECUNIA:11371
# URL:http://secunia.com/advisories/11371

# SECUNIA:11374

# URL:http://secunia.com/advisories/11374

# SECUNIA:11375
# URL:http://secunia.com/advisories/11375

# SECUNIA:11377
# URL:http://secunia.com/advisories/11377

# SECUNIA:11380
# URL:http://secunia.com/advisories/11380

# SECUNIA:11391
# URL:http://secunia.com/advisories/11391

# SECUNIA:11400
# URL:http://secunia.com/advisories/11400

# SECUNIA:11405
# URL:http://secunia.com/advisories/11405

# SECUNIA:11548
# URL:http://secunia.com/advisories/11548

# XF:cvs-rcs-create-files(15864)
# URL:http://xforce.iss.net/xforce/xfdb/15864

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2004-0180

❖ 17653 Apache 2.x PCRE Integer Overflow Vulnerability

A vulnerability has been reported in Apache, which can be exploited by malicious, local users to gain escalated privileges via a specially crafted ".htaccess" file.

The vulnerability has been reported in versions 2.0.35 through 2.0.37, 2.0.39 through 2.0.40, and 2.0.42 through 2.0.54.

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

References:

Initial Advisory:
http://httpd.apache.org/security/vulnerabilities_20.html

Other references:
#SECUNIA:
http://secunia.com/advisories/16688/

#SECUNIA:
http://secunia.com/SA16502/

# DEBIAN:DSA-800

# URL:http://www.debian.org/security/2005/dsa-800

# BID:14620
# URL:http://www.securityfocus.com/bid/14620

# SECTRACK:1014744
# URL:http://securitytracker.com/id?1014744

Product Home Page:
http://httpd.apache.org/

CVE Reference: CAN-2005-2491

❖ 17659 Apache 2.x HTTP Request Smuggling Vulnerability

A vulnerability has been reported in Apache, which can be exploited by malicious people to conduct HTTP request smuggling attacks.

The vulnerability is caused due to an error in the handling of malformed HTTP requests with both "Transfer-Encoding" and "Content-Length" headers and can be exploited to cause Apache to forward malicious HTTP requests in the HTTP body, which will be processed as a separate HTTP requests by the receiving server.

Successful exploitation allows poisoning of the web proxy cache or bypass of certain web application firewall protections, but requires that Apache is configured as a web proxy.

An off-by-one error has also been reported in mod_ssl when printing debug information and configured to use a malicious CRL (Certificate Revocation List).

The vulnerability has been reported in version 2.0.35 through 2.0.37, 2.0.39, 2.0.40, and in version 2.0.42 through 2.0.54.

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

References:

Initial Advisory:
http://httpd.apache.org/security/vulnerabilities_20.html

Other references:
#SECUNIA:
http://secunia.com/advisories/14530/

# MISC:https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=163013

# MANDRAKE:MDKSA-2005:129
# URL:http://www.mandriva.com/security/advisories?name=MDKSA-2005:129

# REDHAT:RHSA-2005:582
# URL:http://rhn.redhat.com/errata/RHSA-2005-582.html

# BUGTRAQ:20050606 A new whitepaper by Watchfire - HTTP Request Smuggling
# URL:http://seclists.org/lists/bugtraq/2005/Jun/0025.html

# MISC:http://www.watchfire.com/resources/HTTP-Request-Smuggling.pdf

# MISC:http://www.securiteam.com/securityreviews/5GP0220G0U.html

# SECTRACK:1014323
# URL:http://securitytracker.com/id?1014323

Product Home Page:
http://httpd.apache.org/

CVE Reference: CAN-2005-1268, CAN-2005-2088

New Vulnerabilities found this Week

- **Microsoft Exchange Server 2003 Folder Listing Denial of Service**
  "Denial of Service"

  A vulnerability has been reported in Microsoft Exchange Server 2003, which can be exploited by malicious users to cause a DoS (Denial of Service).

  The vulnerability is caused due to an unspecified error in the handling of requests to list public folders, and can be exploited to crash the Microsoft Exchange Information Store service (Store.exe) via an IMAP4 request.

  Successful exploitation requires that the following conditions are met:
  * User tries to list public folders using IMAP4 version 4rev1
  * Exchange server does not allow IMAP4 users to list public folders.
  * User does not have a private mailbox on the server.

  References:
  http://support.microsoft.com/kb/840123

- **Cisco IOS Authentication Proxy for FTP/Telnet Buffer Overflow**
  "Denial of Service"

  A vulnerability has been reported in Cisco IOS, 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 when the Authentication Proxy FTP/Telnet is processing user authentication credentials. This can be exploited to cause a buffer overflow.

  Successful exploitation causes a reload of the device and may allow arbitrary code execution, but requires that Authentication Proxy for FTP and/or Telnet Sessions is configured and applied to an active interface.

The vulnerability is reported in the following versions:
* 12.2ZH and 12.2ZL based trains
* 12.3 based trains
* 12.3T based trains
* 12.4 based trains
* 12.4T based trains

References:
http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml
http://www.kb.cert.org/vuls/id/236045

- **Squid "storeBuffer()" Denial of Service Vulnerability**
  "Denial of Service"

  Nickolay has reported a vulnerability in Squid, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

  The vulnerability is caused due to an unspecified error in the use of the "storeBuffer()" function when handling aborted requests. This may be exploited to crash Squid.

  References:
  http://www.squid-cache.org/Versions/v2/2.5/bugs/#squid-2.5.STABLE10-STORE_PENDING

- **mod_ssl "SSLVerifyClient" Security Bypass Security Issue**
  "Bypass client-based certificate authentication and gain unauthorized access"

  A security issue has been reported in mod_ssl, which potentially can be exploited by malicious people to bypass certain security restrictions.

  The security issue is caused due to an error in enforcing client-based certificate authentication ("SSLVerifyClient require") in per-location context, if "SSLVerifyClient optional" was configured in the global virtual host configuration. This may allow malicious people to bypass client-based certificate authentication and gain unauthorized access to certain web pages.

  References:
  http://secunia.com/advisories/16700/

- **DameWare Mini Remote Control Buffer Overflow Vulnerability**
  "Allows execution of arbitrary code"

Jackson Pollocks No5 has discovered a vulnerability in DameWare Mini Remote Control, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error when handling an overly long user ID. This can be exploited to cause a stack-based buffer overflow and allows execution of arbitrary code.

The vulnerability has been confirmed in version 4.8.0.3, and has been reported to affect all versions above 4.0 and prior to 4.9.0.

References:
http://www.jpno5.com/Releases/Public/Exploits/Dameware%20Mini%20Remote%20Control%20Exploit/dameware.txt
http://www.kb.cert.org/vuls/id/170905

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