ScoutNews Team **September 16, 2005**
Issue # 37

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

Keep on eye on all of your IP addresses, news on VOIP security and Spammers sink lower than the Big Easy's sewers.

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

- **Any IP address is a hacker target**

Networked printers, networked thermostats, networked door controllers? Linda LeBlanc explains that any device with an IP address and running some form of Linix or Windows can be compromised.

Hackers can use these machines to launch attacks, store warez, and play games. A common security risk is on systems running a Windows NT kernel. Microsoft is not issuing security patches for NT, yet many older systems are still running embedded NT.

Datamation

Full Story:
http://itmanagement.earthweb.com/entdev/article.php/3547936

❖ VOIP Security; better than you may think

It would appear that reports of VOIP security risks are a bit overblown. Rohan Mahy of IT Architect Magazine reports that most VoIP networks are safer than some would have you believe. Several aspects of VOIP networks actually contribute to a higher level of security over data networks; they are independent of one another and because the vast majority of enterprise VoIP networks don't accept external VoIP calls, those networks are even more protected against spam, phishing, and identity forgery. Also, the very properties of voice, such as the inability to search or skim through content, make it an inherently less interesting target for hackers relative to data files or e-mails.
IT Architect

Full Story:
http://www.itarchitect.com/showArticle.jhtml?articleID=169400802

❖ Spammers further exploit Katrina victims

SurfControl issues a security advisory warning against unsolicited Spam e-mail messages carrying URLs of legitimate donation websites. The Spammers are replicating the donation forms from legitimate charitable organizations.

Simple rule: Legitimate charity organizations are not using unsolicited email to raise contributions.

PRNewswire

Related Links:
http://www.techweb.com/showPressRelease.jhtml?articleID=X367623

New Vulnerabilities Tested in SecureScout

❖ 13277 CVS File Existence Information Disclosure Weakness

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

A weakness has been reported in Concurrent Versions System (CVS), which potentially can be exploited by malicious users to gain knowledge of certain system information.

The problem is caused due to an undocumented switch to the "history" command implemented in "src/history.c". Using the "-X" switch and supplying an arbitrary

filename, CVS will try to access the specified file and returns various information depending on whether the file exists and can be accessed.

This behavior can be exploited to determine the existence and permissions of arbitrary files and directories on a vulnerable system.

The weakness has been reported in version 1.11. Other versions may also be affected.

This issue has been fixed in versions 1.11.17 and 1.12.9.

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

References:

Original advisory:
US-CERT VU#579225:
http://www.kb.cert.org/vuls/id/579225

Other references:
SECUNIA:
URL:http://secunia.com/advisories/12309/

IDEFENSE:20040816 CVS Undocumented Flag Information Disclosure Vulnerability
URL:http://www.idefense.com/application/poi/display?id=130&type=vulnerabilities

CERT-VN:VU#579225
URL:http://www.kb.cert.org/vuls/id/579225

MANDRAKE:MDKSA-2004:108
URL:http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:108

BID:10955
URL:http://www.securityfocus.com/bid/10955

XF:cvs-history-info-disclosure(17001)
URL:http://xforce.iss.net/xforce/xfdb/17001

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

CVE Reference: CAN-2004-0778

❖ 13278 CVS pserver "CVSROOT/passwd" Privilege Escalation Vulnerability

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

A security issue has been identified in CVS, which can be exploited by malicious users to gain escalated privileges.

A user, who has gained write permissions for the "CVSROOT/passwd" file, can execute

arbitrary code with "root" privileges on a system with CVS pserver access enabled.

Issue has been fixed in version 1.11.11 and 1.12.5.

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

References:

Original advisory:

http://ccvs.cvshome.org/servlets/NewsItemView?newsID=88

Other references:

#SECUNIA:

http://secunia.com/advisories/10502/

Product HomePage:

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

CVE Reference: None

❖ 15228 BIND Buffer overflow in DNS resolver functions Vulnerability

The Domain Name System (DNS) provides name, address, and other information about Internet Protocol (IP) networks and devices. By issuing queries to and interpreting responses from DNS servers, IP-enabled network operating systems can access DNS information. When an IP network application needs to access or process DNS information, it calls functions in the stub resolver library, which may be part of the underlying network operating system. On BSD-based systems, DNS stub resolver functions are implemented in the system library libc. In ISC BIND, they are implemented in libbind. On GNU/Linux-based systems, they are implemented in glibc. The DNS resolver libraries on BSD-based systems (libc), ISC BIND (libbind), GNU/Linux (glibc), and possibly other systems that use code derived from ISC BIND contain buffer overflow vulnerabilities in the way the resolver handles DNS responses.

This document specifically addresses a buffer overflow that can ocur when stub resolvers process DNS responses for network name and address resolution.

The stub resolver implementation in ISC BIND 4 (4.8 to 4.9.8 at least) is vulnerable to buffer overflows via DNS responses for both network and host name and address resolution. The BSD and GNU/Linux stub resolvers are derived from the BIND 4 code, therefore they are also vulnerable via both sets of responses.

* In October 1999, GNU/Linux glibc was patched against the buffer overflow that can occur during the processing of responses for host name and address resolution. glibc versions 2.1.3 and later are not vulnerable to this problem.
* In June 2002, ISC BIND and {Free,Net,Open}BSD patched their stub resolver libraries against both problems. At this time, it was discovered that glibc was still vulnerable to a buffer overflow via responses for network name and address resolution. Unpatched

versions of GNU glibc 2.2.5 and earlier are vulnerable to this problem.

The Systems Affected section of this document only applies to products that use the GNU/Linux stub resolver implementation in glibc. See CERT Advisory CA-2002-19 and VU#803539 for more complete vendor information.

Note that any application that uses a vulnerable resolver library is likely to be affected. Applications that are statically linked must be recompiled using patched resolver libraries.

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

References:

Original Advisory:

http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:

REDHAT:RHSA-2002:139

URL:http://rhn.redhat.com/errata/RHSA-2002-139.html

BUGTRAQ:20020704 Re: Remote buffer overflow in resolver code of libc

URL:http://marc.theaimsgroup.com/?l=bugtraq&m=102581482511612&w=2

SUSE:SuSE-SA:2002:026

CERT:CA-2002-19

CERT-VN:VU#542971

URL:http://www.kb.cert.org/vuls/id/542971

MANDRAKE:MDKSA-2002:050

URL:http://www.linux-mandrake.com/en/security/2002/MDKSA-2002-050.php

CONECTIVA:CLSA-2002:507

URL:http://distro.conectiva.com/atualizacoes/?id=a&anuncio=000507

Product HomePage:

http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CAN-2002-0684

❖ 15229 BIND SIGINT and SIGIOT symlink Vulnerability

The named daemon will dump the named database to /var/tmp/named_dump.db when it receives a SIGINT signal. It does not check for symbolic links while doing so and can be made to overwrite any file in the system.

The named daemons will append named statistics to /var/tmp/named.stats when it receives a SIGIOT signal. It does not check for symbolic links while doing so and ca be made to append to any file in the system.

BIND 8.1.x is not vulnerable as it uses a private directory specified in named.{boot,conf} for temporary and debug dumps.

Issue affects BIND versions up to 4.9.7.

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

References:

Original Advisory:

http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:

BUGTRAQ:19980410 BIND 4.9.7 named follows symlinks, clobbers anything

URL:http://www.securityfocus.com/archive/1/8966

BID:80

URL:http://www.securityfocus.com/bid/80

Product HomePage:

http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CAN-1999-1499

❖ 15230 BIND 4 and 8.2.x stub resolver libraries maximum buffer size Vulnerability

The BIND 4 and BIND 8.2.x stub resolver libraries, and other libraries such as glibc 2.2.5 and earlier, libc, and libresolv, use the maximum buffer size instead of the actual size when processing a DNS response, which causes the stub resolvers to read past the actual boundary ("read buffer overflow"), allowing remote attackers to cause a denial of service (crash).

The issue affects versions 8.2.x lower than 8.2.7

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
FREEBSD:FreeBSD-SA-02:42
MANDRAKE:MDKSA-2004:009
NETBSD:NetBSD-SA2002-015
REDHAT:RHSA-2002:197
URL:http://rhn.redhat.com/errata/RHSA-2002-197.html

REDHAT:RHSA-2002:258
REDHAT:RHSA-2003:022
REDHAT:RHSA-2003:212
URL:http://rhn.redhat.com/errata/RHSA-2002-197.html
CERT-VN:VU#738331
URL:http://www.kb.cert.org/vuls/id/738331
XF:dns-resolver-lib-read-bo(10295)
CONECTIVA:CLA-2002:535

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-2002-1146

❖ 15231 BIND DNS resolver code buffer overflow Vulnerability

The Domain Name System (DNS) provides name, address, and other information about Internet Protocol (IP) networks and devices. By issuing queries to and interpreting responses from DNS servers, IP-enabled network operating systems can access DNS information. When an IP network application needs to access or process DNS information, it calls functions in the stub resolver library, which may be part of the underlying network operating system. On BSD-based systems, DNS stub resolver functions are implemented in the system library libc. In ISC BIND, they are implemented in libbind, and on GNU/Linux-based systems, they are implemented in glibc.

The DNS resolver libraries on BSD-based systems (libc), ISC BIND (libbind), GNU/Linux (glibc), and possibly other systems that use code derived from ISC BIND contain buffer overflow vulnerabilities in the way the resolvers handle DNS responses. Quoting from FreeBSD Security Advisory FreeBSD-SA-02:28.resolv:

DNS messages have specific byte alignment requirements, resulting in padding in messages. In a few instances in the resolver code, this padding is not taken into account when computing available buffer space. As a result, the parsing of a DNS message may result in a buffer overrun of up to a few bytes for each record included in the message.

NetBSD Security Advisory 2002-006 provides further detail:

In lib/libc/net/gethnamaddr.c:getanswer() and lib/libc/net/getnetnamadr.c:getnetanswer(), two variables manage packet buffer parsing - a pointer to the byte we are looking at, and the remaining length on the buffer. The remaining length was not updated consistently, and malicious DNS responses are able to write outside the buffer.

This problem is not limited to DNS servers or to BIND. Any application that uses a vulnerable resolver library is likely to be affected. Applications that are statically linked must be recompiled using patched resolver libraries.

Note that the DNS stub resolver implemented in glibc on GNU/Linux systems is vulnerable via DNS lookups for network names and addresses (VU#542971).

The issue affects versions 9.2.x lower than 9.2.2.
The issue affects versions 8.2.x lower than 8.2.6.

The issue affects versions 8.1.x lower than 8.1.3.
The issue affects versions 4.9.x lower than 4.9.9.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
BUGTRAQ:20020626 Remote buffer overflow in resolver code of libc
NTBUGTRAQ:20020703 Buffer overflow and DoS i BIND
MISC:http://www.pine.nl/advisories/pine-cert-20020601.txt
CERT:CA-2002-19
CERT-VN:VU#803539
URL:http://www.kb.cert.org/vuls/id/803539
AIXAPAR:IY32719
AIXAPAR:IY32746
CALDERA:CSSA-2002-SCO.37
CALDERA:CSSA-2002-SCO.39
CONECTIVA:CLSA-2002:507
ENGARDE:ESA-20020724-018
FREEBSD:FreeBSD-SA-02:28
MANDRAKE:MDKSA-2002:038
MANDRAKE:MDKSA-2002:043
NETBSD:NetBSD-SA2002-006
REDHAT:RHSA-2002:119
REDHAT:RHSA-2002:133
REDHAT:RHSA-2002:139
REDHAT:RHSA-2002:167
REDHAT:RHSA-2003:154
SGI:20020701-01-I
BUGTRAQ:20020704 [OpenPKG-SA-2002.006] OpenPKG Security Advisory (bind)
XF:dns-resolver-lib-bo(9432)
BID:5100

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-2002-0651

❖ 15232 BIND SRV record denial of service Vulnerability

This vulnerability can cause affected DNS servers running named to go into an infinite loop, thus preventing further name requests to be handled. This can happen if an SRV record (defined in RFC2782) is sent to the vulnerable server.

The vulnerability can be used by malicious users to break the DNS services being offered at all exposed sites on the Internet. System administrators are strongly recommended to upgrade their DNS software with either ISC's current distribution or their vendor-supplied software. See the Solution and Vendor Information sections of this document for more details.

The issue affects version 8.2 through 8.2.2-P6.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
CERT:CA-2000-20
REDHAT:RHSA-2000:107
MANDRAKE:MDKSA-2000:067
CONECTIVA:CLSA-2000:338
CONECTIVA:CLSA-2000:339
DEBIAN:20001112 bind: remote Denial of Service
IBM:ERS-SVA-E01-2000:005.1
SUSE:SuSE-SA:2000:45
XF:bind-srv-dos(5814)

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-2000-0888

❖ 15683 Mozilla IDN URL Domain Name Buffer Overflow (Remote File Checking)

Tom Ferris has discovered a vulnerability in Mozilla, which can be exploited by malicious people to cause a DoS (Denial of Service) or to compromise a user's system.

The vulnerability is caused due to an error in the handling of an IDN URLs that contains the 0xAD character in its domain name. This can be exploited to cause a heap-based buffer overflow.

Successful exploitation crashes Mozilla and may allow code execution but requires that the user is tricked into visiting a malicious web site or open a specially crafted HTML file.

The vulnerability has been confirmed in version 1.7.11. Prior versions are reportedly also affected.

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

References:

Original Advisories:
http://security-protocols.com/advisory/sp-x17-advisory.txt
https://addons.mozilla.org/messages/307259.html

Other references:

US-CERT VU#573857:

URL:http://www.kb.cert.org/vuls/id/573857

FULLDISC:20050909 Mozilla Firefox "Host:" Buffer Overflow
URL:http://marc.theaimsgroup.com/?l=full-disclosure&m=112624614008387&w=2

MISC:http://www.security-protocols.com/firefox-death.html

MISC:http://www.security-protocols.com/advisory/sp-x17-advisory.txt

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

CVE Reference: CAN-2005-2871

❖ 15684 Netscape IDN URL Domain Name Buffer Overflow (Remote File Checking)

Tom Ferris has discovered a vulnerability in Netscape, which can be exploited by malicious people to cause a DoS (Denial of Service) or to compromise a user's system.

The vulnerability is caused due to an error in the handling of an IDN URLs that contains the 0xAD character in its domain name. This can be exploited to cause a heap-based buffer overflow.

Successful exploitation crashes Netscape and may allow code execution but requires that the user is tricked into visiting a malicious web site or open a specially crafted HTML file.

The vulnerability has been confirmed in versions 8.0.3.3 and 7.2. Other versions may also be affected.

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

References:

Original Advisories:
http://security-protocols.com/advisory/sp-x17-advisory.txt
https://addons.mozilla.org/messages/307259.html

Other references:

US-CERT VU#573857:
URL:http://www.kb.cert.org/vuls/id/573857

FULLDISC:20050909 Mozilla Firefox "Host:" Buffer Overflow
URL:http://marc.theaimsgroup.com/?l=full-disclosure&m=112624614008387&w=2

MISC:http://www.security-protocols.com/firefox-death.html

MISC:http://www.security-protocols.com/advisory/sp-x17-advisory.txt

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

CVE Reference: CAN-2005-2871

- **15685 Firefox IDN URL Domain Name Buffer Overflow (Remote File Checking)**

Tom Ferris has discovered a vulnerability in Firefox, which can be exploited by malicious people to cause a DoS (Denial of Service) or to compromise a user's system.

The vulnerability is caused due to an error in the handling of an IDN URLs that contains the 0xAD character in its domain name. This can be exploited to cause a heap-based buffer overflow.

Successful exploitation crashes Firefox and may allow code execution but requires that the user is tricked into visiting a malicious web site or open a specially crafted HTML file.

The vulnerability has been confirmed in version 1.0.6, and is reported to affect versions prior to 1.0.6, and version 1.5 Beta 1.

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

References:

Original Advisories:
http://security-protocols.com/advisory/sp-x17-advisory.txt
https://addons.mozilla.org/messages/307259.html

Other references:

US-CERT VU#573857:
URL:http://www.kb.cert.org/vuls/id/573857

FULLDISC:20050909 Mozilla Firefox "Host:" Buffer Overflow
URL:http://marc.theaimsgroup.com/?l=full-disclosure&m=112624614008387&w=2

MISC:http://www.security-protocols.com/firefox-death.html

MISC:http://www.security-protocols.com/advisory/sp-x17-advisory.txt

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

CVE Reference: CAN-2005-2871

New Vulnerabilities found this Week

- **IBM Lotus Domino "BaseTarget" and "Src" Cross-Site Scripting**

"Cross-site scripting attacks"

Two vulnerabilities have been reported in Lotus Domino, which can be

exploited by malicious people to conduct cross-site scripting attacks.

Input passed to the "BaseTarget" and "Src" parameters isn't properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerabilities have been reported in version 6.5.2. Other versions may also be affected.

References:
http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg1LO07850&loc=en_US&cs=utf-8&cc=us&lang=all
http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg1LO07849&loc=en_US&cs=utf-8&cc=us&lang=all

- **Apple Mac OS X update for Java**

"Disclose sensitive information and gain escalated privileges"

Some vulnerabilities have been reported in Java for Mac OS X, which can be exploited by malicious, local users to manipulate certain data, disclose sensitive information and gain escalated privileges, and by malicious people to bypass certain security restrictions.

1) An unspecified error in the handling of temporary files can be exploited in combination with a race condition to corrupt or create arbitrary files.

2) An error in the privileged helper where temporary files are insecurely created can be exploited to corrupt or create arbitrary files.

This does not affect systems prior to Mac OS X 10.4.

3) An unspecified error in the utility used for updating Java shared archives can be exploited by malicious, local users to gain escalated privileges.

This does not affect systems prior to Mac OS X 10.4.

4) An unspecified error in the use of Mac OS X specific extensions can be exploited by untrusted malicious applets to gain escalated privileges.

This does not affect systems prior to Mac OS X 10.4.

5) The problem is that a Java ServerSocket object can be created for a port which is in use. This can be exploited to intercept traffic sent to a Java application already listening on that port.

This does not affect systems prior to Mac OS X 10.4.

This update also fixes some issues in Java that aren't specific to Mac OS X.

References:
http://docs.info.apple.com/article.html?artnum=302265
http://docs.info.apple.com/article.html?artnum=302266

- **Linksys WRT54G Multiple Vulnerabilities**

"Denial of Service"

Greg MacManus has reported some vulnerabilities in WRT54G, which can be exploited malicious people to bypass certain security restrictions, cause a DoS (Denial of Service), or compromise a vulnerable system.

1) A validation error exists in the "POST" method handlers of the built-in web management httpd server when handing a negative "Content-Length" value. This can be exploited to cause the httpd to become unresponsive, and may cause the web management interface to be unavailable.

The vulnerability has been reported in firmware version 3.01.3, 3.03.6 and 4.00.7. All versions prior to 4.20.7 may also be affected.

2) A design error in upgrade.cgi can be exploited by an unauthenticated user to upload arbitrary firmware onto the router. The uploaded firmware will be saved on the router but will not take effect until the router is rebooted.

The vulnerability has been reported in firmware version 3.01.3, 3.03.6 and 4.00.7. All versions prior to 4.20.7 may also be affected.

3) A design error in restore.cgi can be exploited by an unauthenticated user to upload arbitrary configuration settings to router. The uploaded configuration settings will be saved on the router but will not take effect until the router is rebooted.

The vulnerability has been reported in firmware version 3.01.3, 3.03.6 and 4.00.7. All versions prior to 4.20.7 may also be affected.

4) The vulnerability is caused due to a boundary error in apply.cgi when sending a POST request to the page with a content length longer than 10000 bytes. This can be exploited to crash httpd and cause the web management interface to become unavailable, and may allow code execution with root privileges.

The vulnerability has been reported in firmware version 3.01.3 and 3.03.6. All versions prior to 4.20.7 may also be affected.

5) An authentication error in ezconfig.asp can be exploited by unauthenticated users to upload configuration settings to a vulnerable device if the fixed 256-byte XOR key used to encrypt the settings is known.

The vulnerability has been reported in firmware version 3.01.3 and 3.03.6.

Successful exploitation of the vulnerabilities requires the ability to connect to the web management interface.

References:
http://www.idefense.com/application/poi/display?id=308&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=307&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=306&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=305&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=304&type=vulnerabilities

- **Sun Java System Application Server JAR File Content Disclosure**

"Disclose certain sensitive information"

A vulnerability has been reported in Sun Java System Application Server, which can be exploited by malicious people to disclose certain sensitive information.

The vulnerability is caused due to an unspecified error that allows the contents of a JAR file of a deployed web application to be exposed.

The vulnerability has been reported in the following versions:
* Platform Edition 8.1 2005Q1
* Platform Edition 8.1 2005Q1 (UR1) Update Release 1
* Enterprise Edition 8.1 2005Q1

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101905-1&searchclause

- **PHP-Nuke SQL Injection Vulnerabilities**

"SQL injection attacks"

Robin Verton has discovered some vulnerabilities in PHP-Nuke, which can be exploited by malicious people to conduct SQL injection attacks.

Input passed to the "name", "sid", and "pid" parameters in "modules.php" sent via a POST request isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerabilities have been confirmed in version 7.7. Version 7.8 and prior are reportedly also be affected.

References:
http://secunia.com/advisories/16801/

- **Firefox IDN URL Domain Name Buffer Overflow**

"Denial of Service"

Tom Ferris has discovered a vulnerability in Firefox, which can be exploited by malicious people to cause a DoS (Denial of Service) or to compromise a user's system.

The vulnerability is caused due to an error in the handling of an IDN URLs that contains the 0xAD character in its domain name. This can be exploited to cause a heap-based buffer overflow.

Successful exploitation crashes Firefox and may allow code execution but requires that the user is tricked into visiting a malicious web site or open a specially crafted HTML file.

The vulnerability has been confirmed in version 1.0.6, and is reported to affect versions prior to 1.0.6, and version 1.5 Beta 1.

References:
http://security-protocols.com/advisory/sp-x17-advisory.txt
https://addons.mozilla.org/messages/307259.html
http://www.kb.cert.org/vuls/id/573857

- **Cisco CSS SSL Authentication Bypass Vulnerability**

"Bypass certain security restrictions"

A vulnerability has been reported in Cisco CSS (Content Services Switch), which can be exploited by malicious users to bypass certain security restrictions.

The vulnerability is caused due to an error in handling the situation when SSL clients fail to renegotiate the SSL session. This can be exploited to bypass client certificate authentication and may allow access to protected content.

Successful exploitation requires that client authentication using SSL certificates is enabled.

The vulnerability has been reported in the following products:
* Cisco CSS 11500 Series Content Services Switches with the CSS5-SSL-K9 SSL module
* Cisco 11501 Content Services Switch with SSL (CSS11501S-K9)

References:
http://www.cisco.com/warp/public/707/cisco-sn-20050908-css.shtml

- **Linux Kernel Multiple Vulnerabilities**

"Denial of Service and gain escalated privileges"

Some vulnerabilities have been reported in the Linux kernel, which potentially can be exploited by malicious, local users to disclose certain sensitive information, cause a DoS (Denial of Service) and gain escalated privileges, or by malicious people to cause a DoS.

1) A boundary error in "sendmsg()" when copying 32bit "msg_control" contents from user-space to the kernel can be exploited to cause a buffer overflow. This may allow a malicious user to gain root privileges and execute arbitrary code with kernel privileges.

The vulnerability has been reported in version 2.4.21 and 2.6.9. Other versions may also be affected.

2) An error in the "raw_sendmsg()" function may allow a malicious user to read kernel memory contents and disclose certain information, or to manipulate certain hardware state to cause a DoS.

The vulnerability has been reported in the 2.6 kernel branch.

3) An error in performing boundary checks in the standard multi-block cipher processors can be exploited to cause a kernel panic in an IPSec environment when handling packets with a block size that is not multiple of "bsize".

The vulnerability has been reported in version 2.6.13. Prior versions may also be affected.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13.1

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