netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 17

May 4, 2007

Table of Contents

Product Focus

Apache Chunked Vulnerability Scanner – The Apache Chunked Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Apache Chunked Encoding buffer overflow.

This Week in Review

Security and removable medias. Online banking with card reader. DDoS not so popular anymore. Let's look at the hype.

Enjoy reading & Stay safe.

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

Top Security News Stories this Week

- **Secure The Smallest Endpoints**

Securing USB drives and other types of removable media is one of the top priorities for security administrators today. These devices are vulnerable because most removable media don't have built-in data protection and because they connect so easily to computers connected to corporate networks.

Fortunately, there are technologies and strategies available today that can help your

small to medium-sized enterprise mitigate the risks from removable media. Let's take a look.
Most industry watchers believe the proliferation of unsecured endpoints is a pressing problem that merits immediate attention. John Jefferies, vice president of marketing at RedCannon (www.Processor.com/Red_Cannon), a provider of centrally managed, secure mobile-access solutions for the enterprise, says the problem is huge.

"Connecting with a USB device alone can turn a single endpoint into an unprotected gateway to the entire network, putting intellectual property and private corporate and customer data at risk," says Jefferies.

processor

Full Story :
http://www.processor.com/editorial/article.asp?Article=articles/p2918/30p18/30p18.asp&GUID=40C1B2038EA04F78907C709CC55B7B18

❖ Royal Bank of Scotland rolls out chip and PIN

The Royal Bank of Scotland is dishing out chip and PIN devices to its online banking customers.

The chip and PIN card readers will be sent to customers free of charge and people will start receiving the devices this week.

An Royal Bank of Scotland (RBS) spokeswoman said that customers who make frequent "advanced transactions" — people setting up payments to new third-party accounts, setting up new standing order payees or changing online banking PINs or passwords — will be the first to receive the devices.

The spokeswoman said: "The aim of the project is that all our customers who use online banking will eventually have a card reader."

zdnet

Full Story :
http://news.zdnet.co.uk/security/0,1000000189,39286964,00.htm

❖ Hackers shy away from DDoS attacks

The quantity of distributed denial-of-service attacks launched for the purpose of extortion has fallen, according to security vendor Symantec.

A distributed denial-of-service (DDoS) attack uses a network of compromised computers, known as a botnet, to send a large number of packets to a site, causing its server to fall over. Some attackers try to extort money from the site by threatening to launch another attack. However, DDoS attacks are becoming less frequent because of increasing risks to attackers, according to Symantec.
"In the last six months of 2006 we saw a pretty sharp decline in the daily number of denial-of-service attacks. Although there are likely a number of factors at play here, I think there is one primary factor: denial-of-service extortion attacks are no longer profitable," wrote

the vendor's security response engineer Yazan Gable in a blog post.

zdnet

Full Story :
http://news.zdnet.co.uk/security/0,1000000189,39286941,00.htm

- **Don't Believe the Hype: The 21 Biggest Technology Flops**

We fondly recall 21 overpromoted products and technologies that utterly failed to live up to their hype -- and we give you a chance to choose the biggest flop of all.
Hype is the coin of the realm in the technology business. If you listen to vendors and the media, it may sometimes seem as though every new product, service, concept or even security threat will be the Next Big Thing. Some live up to all the fuss, but many don't -- and some fail spectacularly.

Take the Michelangelo virus, the subject of a media frenzy 15 years ago. March 6, 1992, was the day that the dreaded virus was supposed to strike. Journalists went overboard covering this virus, which had supposedly burrowed itself into hard drives around the world throughout 1991 and was set to start destroying data on March 6, the birthday of the famous artist.

It didn't happen that way, of course: Damage was minimal. But in honor of Michelangelo's birthday, we thought we'd track down history's biggest technology flops.

Here we nominate 21 of our favorite overhyped failures, presented in alphabetical order. At the end of the piece, we'll ask you to vote on which is the biggest tech flop of them all, or write in a nominee of your own.

computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9012345

New Vulnerabilities Tested in SecureScout

- **16491 Vulnerability QuickTime Java Extension "toQTPointer()" Code Execution (Remote File Checking)**

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

The vulnerability is caused due to an input validation error in "toQTPointer()" within the QuickTime Java extensions (QTJava.dll) and can be exploited to write arbitrary values to memory locations outside of an allocated buffer.

Successful exploitation allows execution of arbitrary code when a user visits a malicious web site using a Java-enabled browser e.g. Safari, Internet Explorer, or Firefox.

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

References:

Original Advisory:
http://docs.info.apple.com/article.html?artnum=305446

Other references:
MISC: http://cansecwest.com/post/2007-04-20-14:54:00.First_Mac_Hacked_Cancel_Or_Allow
MISC: http://www.matasano.com/log/812/breaking-macbook-vuln-in-quicktime-affects-win32-apple-code/
MISC: http://www.matasano.com/log/806/hot-off-the-matasano-sms-queue-cansec-macbook-challenge-won/
MISC: http://www.theregister.co.uk/2007/04/20/pwn-2-own_winner/
MISC: http://www.zerodayinitiative.com/advisories/ZDI-07-023.html
APPLE:APPLE-SA-2007-05-01
URL:http://lists.apple.com/archives/security-announce/2007/May/msg00001.html
SECTRACK:1017950
URL:http://www.securitytracker.com/id?1017950
XF:quicktime-unspecified-code-execution(33827)
URL:http://xforce.iss.net/xforce/xfdb/33827

Product:
http://www.apple.com/quicktime/

CVE Reference: CVE-2007-2175

❖ 16490 ProFTPD Auth API Multiple Authentication Modules Security Issue

ProFTPD is an FTP server available for many Unix platforms.

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

The security issue is caused due to an error within ProFTPD's Auth API. If multiple authentication modules are used, it is possible that one module provides data, which is then authenticated against another module. This can e.g. be exploited to bypass certain security restrictions if authentication modules are configured with different policies.

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

References:

Original Advisory:
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=419255

Other references:
CONFIRM: http://bugs.proftpd.org/show_bug.cgi?id=2922
BID:23546
URL:http://www.securityfocus.com/bid/23546
FRSIRT:ADV-2007-1444

URL:http://www.frsirt.com/english/advisories/2007/1444
SECTRACK:1017931
URL:http://securitytracker.com/id?1017931
SECUNIA:24867
URL:http://secunia.com/advisories/24867
XF:proftpd-authapi-security-bypass(33733)
URL:http://xforce.iss.net/xforce/xfdb/33733

Product page:
http://www.proftpd.org/

CVE Reference: CVE-2007-2165

❖ 12151 PostgreSQL SECURITY DEFINER Functions Privilege Escalation Vulnerability

A security issue has been reported in PostgreSQL, which potentially can be exploited by malicious users to gain escalated privileges.

The security issue is caused due to an error in SECURITY DEFINER functions and can be exploited to gain escalated privileges by modifying the search_path and using temporary objects.

PostgreSQL versions prior to 8.2.4, 8.1.9, 8.0.13, 7.4.17, or 7.3.19 are vulnerable to these issues.

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

References:

Original advisory:
http://www.postgresql.org/about/news.791

Other references:
CONFIRM: http://www.postgresql.org/support/security.html
CONFIRM: https://issues.rpath.com/browse/RPL-1292
MANDRIVA:MDKSA-2007:094
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:094
SUNALERT:102894
URL:http://sunsolve.sun.com/search/document.do?assetkey=1-26-102894-1
TRUSTIX:2007-0015
URL:http://www.trustix.org/errata/2007/0015/
UBUNTU:USN-454-1
URL:http://www.ubuntu.com/usn/usn-454-1
BID:23618
URL:http://www.securityfocus.com/bid/23618
FRSIRT:ADV-2007-1497
URL:http://www.frsirt.com/english/advisories/2007/1497
FRSIRT:ADV-2007-1549
URL:http://www.frsirt.com/english/advisories/2007/1549
SECTRACK:1017974
URL:http://www.securitytracker.com/id?1017974

SECUNIA:25019
URL:http://secunia.com/advisories/25019
SECUNIA:25005
URL:http://secunia.com/advisories/25005
SECUNIA:24989
URL:http://secunia.com/advisories/24989
SECUNIA:25037
URL:http://secunia.com/advisories/25037
SECUNIA:24999
URL:http://secunia.com/advisories/24999
SECUNIA:25058
URL:http://secunia.com/advisories/25058
XF:postgresql-searchpath-privilege-escalation(33842)
URL:http://xforce.iss.net/xforce/xfdb/33842

Home page:
http://www.postgresql.org/

CVE Reference: CVE-2007-2138

❖ 16489 bftpd GET/MGET File Transfer Denial of Service Vulnerability

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

The vulnerability is caused due to a double-free error when sending files. This can be exploited to cause a DoS via unspecified vectors using the GET or MGET commands.

The vulnerability is reported in versions prior to 1.8. Other versions may also be affected.

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

References:

Original Advisory:
http://bftpd.sourceforge.net/downloads/CHANGELOG
http://bftpd.sourceforge.net/

Other references:
BID:23406
URL:http://www.securityfocus.com/bid/23406
FRSIRT:ADV-2007-1347
URL:http://www.frsirt.com/english/advisories/2007/1347
SECUNIA:24864
URL:http://secunia.com/advisories/24864
XF:bftpd-getmget-dos(33594)
URL:http://xforce.iss.net/xforce/xfdb/33594

Product page:
http://bftpd.sourceforge.net/

CVE Reference: CVE-2007-2010

❖ 16487 Winamp libsndfile.dll MAT File Handling NULL Byte Overwrite (Remote File Checking)

Piotr Bania has discovered a vulnerability in Winamp, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error within the LIBSNDFILE.DLL library when handling Matlab version 4.2 files. This can be exploited to overwrite an arbitrary memory location with a NULL byte when opening a specially crafted MAT file.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is confirmed in version 5.33. Other versions and applications that use the library may also be affected.

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

References:

Original advisory:
http://www.piotrbania.com/all/adv/nullsoft-winamp-libsndfile-adv.txt

Other references:
BUGTRAQ:20070406 AOL Nullsoft Winamp LIBSNDFILE.DLL Remote Memory Corruption (Off By Zero)
URL:http://www.securityfocus.com/archive/1/archive/1/464889/100/0/threaded
MLIST:[dailydave] 20070406 AOL Nullsoft Winamp LIBSNDFILE.DLL Remote Memory Corruption (Off By Zero)
URL:http://marc.info/?l=dailydave&m=117589848432659&w=2
BID:23351
URL:http://www.securityfocus.com/bid/23351
FRSIRT:ADV-2007-1286
URL:http://www.frsirt.com/english/advisories/2007/1286
SECTRACK:1017886
URL:http://www.securitytracker.com/id?1017886
SECUNIA:24766
URL:http://secunia.com/advisories/24766
XF:winamp-libsndfile-code-execution(33481)
URL:http://xforce.iss.net/xforce/xfdb/33481

Product homepage:
http://www.winamp.com/

CVE Reference: CVE-2007-1921

❖ 16485 Wireshark MIME Multipart dissector Denial of Service Vulnerability (Remote File Checking)

Off-by-one error in the MIME Multipart dissector in Wireshark (formerly Ethereal) 0.10.1

through 0.99.3 allows remote attackers to cause a denial of service (crash) via certain vectors that tragger an assertion error related to unexpected length values.

The vulnerability has been reported in versions 0.10.1 to 0.99.3.

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

References:

Original Advisory:
http://www.wireshark.org/security/wnpa-sec-2006-03.html

Other references:
BUGTRAQ:20061101 rPSA-2006-0202-1 tshark wireshark
URL:http://www.securityfocus.com/archive/1/archive/1/450307/100/0/threaded
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-03.html
CONFIRM: https://issues.rpath.com/browse/RPL-746
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-255.htm
DEBIAN:DSA-1201
URL:http://www.us.debian.org/security/2006/dsa-1201
MANDRIVA:MDKSA-2006:195
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2006:195
REDHAT:RHSA-2006:0726
URL:http://www.redhat.com/support/errata/RHSA-2006-0726.html
SGI:20061101-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P
SUSE:SUSE-SA:2006:065
URL:http://www.novell.com/linux/security/advisories/2006_65_ethereal.html
BID:20762
URL:http://www.securityfocus.com/bid/20762
FRSIRT:ADV-2006-4220
URL:http://www.frsirt.com/english/advisories/2006/4220
SECTRACK:1017129
URL:http://securitytracker.com/id?1017129
SECUNIA:22590
URL:http://secunia.com/advisories/22590
SECUNIA:22692
URL:http://secunia.com/advisories/22692
SECUNIA:22659
URL:http://secunia.com/advisories/22659
SECUNIA:22672
URL:http://secunia.com/advisories/22672
SECUNIA:22797
URL:http://secunia.com/advisories/22797
SECUNIA:22841
URL:http://secunia.com/advisories/22841
SECUNIA:22929
URL:http://secunia.com/advisories/22929
SECUNIA:23096
URL:http://secunia.com/advisories/23096
XF:wireshark-mime-dos(29844)
URL:http://xforce.iss.net/xforce/xfdb/29844

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2006-4574

❖ 16484 Wireshark WBXML dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the WBXML dissector in Wireshark (formerly Ethereal) 0.10.11 through 0.99.3 allows remote attackers to cause a denial of service (crash) via certain vectors that trigger a null dereference.

The vulnerability has been reported in versions 0.10.11 to 0.99.3.

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

References:

Original Advisory:
http://www.wireshark.org/security/wnpa-sec-2006-03.html

Other references:
BUGTRAQ:20061101 rPSA-2006-0202-1 tshark wireshark
URL:http://www.securityfocus.com/archive/1/archive/1/450307/100/0/threaded
CONFIRM: https://issues.rpath.com/browse/RPL-746
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-255.htm
MANDRIVA:MDKSA-2006:195
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2006:195
REDHAT:RHSA-2006:0726
URL:http://www.redhat.com/support/errata/RHSA-2006-0726.html
SGI:20061101-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P
SUSE:SUSE-SA:2006:065
URL:http://www.novell.com/linux/security/advisories/2006_65_ethereal.html
BID:20762
URL:http://www.securityfocus.com/bid/20762
FRSIRT:ADV-2006-4220
URL:http://www.frsirt.com/english/advisories/2006/4220
SECTRACK:1017129
URL:http://securitytracker.com/id?1017129
SECUNIA:22590
URL:http://secunia.com/advisories/22590
SECUNIA:22692
URL:http://secunia.com/advisories/22692
SECUNIA:22672
URL:http://secunia.com/advisories/22672
SECUNIA:22797
URL:http://secunia.com/advisories/22797
SECUNIA:22841
URL:http://secunia.com/advisories/22841
SECUNIA:22929
URL:http://secunia.com/advisories/22929
SECUNIA:23096
URL:http://secunia.com/advisories/23096
XF:wireshark-wbxml-dos(29842)

URL:http://xforce.iss.net/xforce/xfdb/29842

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2006-5469

❖ 16483 Wireshark XOT dissector Denial of Service Vulnerability (Remote File Checking)

epan/dissectors/packet-xot.c in the XOT dissector (dissect_xot_pdu) in Wireshark (formerly Ethereal) 0.9.8 through 0.99.3 allows remote attackers to cause a denial of service (memory consumption and crash) via an encoded XOT packet that produces a zero length value when it is decoded.

The vulnerability has been reported in versions 0.9.8 to 0.99.3.

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

References:

Original Advisory:
http://www.wireshark.org/security/wnpa-sec-2006-03.html

Other references:
BUGTRAQ:20061101 rPSA-2006-0202-1 tshark wireshark
URL:http://www.securityfocus.com/archive/1/archive/1/450307/100/0/threaded
CONFIRM: https://issues.rpath.com/browse/RPL-746
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-255.htm
DEBIAN:DSA-1201
URL:http://www.us.debian.org/security/2006/dsa-1201
MANDRIVA:MDKSA-2006:195
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2006:195
REDHAT:RHSA-2006:0726
URL:http://www.redhat.com/support/errata/RHSA-2006-0726.html
SGI:20061101-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P
SUSE:SUSE-SA:2006:065
URL:http://www.novell.com/linux/security/advisories/2006_65_ethereal.html
CERT-VN:VU#723736
URL:http://www.kb.cert.org/vuls/id/723736
BID:20762
URL:http://www.securityfocus.com/bid/20762
FRSIRT:ADV-2006-4220
URL:http://www.frsirt.com/english/advisories/2006/4220
SECTRACK:1017129
URL:http://securitytracker.com/id?1017129
SECUNIA:22590
URL:http://secunia.com/advisories/22590
SECUNIA:22692
URL:http://secunia.com/advisories/22692
SECUNIA:22659
URL:http://secunia.com/advisories/22659
SECUNIA:22672

URL:http://secunia.com/advisories/22672
SECUNIA:22797
URL:http://secunia.com/advisories/22797
SECUNIA:22841
URL:http://secunia.com/advisories/22841
SECUNIA:22929
URL:http://secunia.com/advisories/22929
SECUNIA:23096
URL:http://secunia.com/advisories/23096
XF:wireshark-xot-dos(29843)
URL:http://xforce.iss.net/xforce/xfdb/29843

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2006-4805

❖ 16476 CMS Cross-Site Scripting and Spoofing Vulnerability (MS07-018/925939) (Remote File Checking)

A cross-site scripting and spoofing vulnerability exists in Microsoft Content Management Server (MCMS) which could allow an attacker to convince a user to run a malicious script. If this malicious script is run, it would execute in the security context of the user. Attempts to exploit this vulnerability require user interaction. This vulnerability could allow an attacker access to any data on the affected systems that was accessible to the individual user.

It may also be possible for an attacker to exploit this vulnerability to modify Web browser caches and intermediate proxy server caches, and put spoofed content in those caches.

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

References:

Original advisory:
MS07-018
http://www.microsoft.com/technet/security/bulletin/ms07-018.mspx

CVE Reference: CVE-2007-0939

❖ 16475 CMS Memory Corruption Vulnerability (MS07-018/925939) (Remote File Checking)

A remote code execution vulnerability exists in Content Management Server because of the way that it handles a specially crafted HTTP request.

An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

Original advisory:
MS07-018
http://www.microsoft.com/technet/security/bulletin/ms07-018.mspx

CVE Reference: CVE-2007-0938

New Vulnerabilities found this Week

Winamp MP4 File Handling Memory Corruption Vulnerability
"Execution of arbitrary code"

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

The vulnerability is caused due to an error within the handling of MP4 files and can be exploited to cause memory corruption via a specially crafted MP4 file.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in version 5.34. Other versions may also be affected.

References:
http://milw0rm.com/exploits/3823

Adobe Products PNG.8BI PNG File Handling Buffer Overflow
"Execution of arbitrary code"

Marsu has discovered a vulnerability in various Adobe Products, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the PNG.8BI Photoshop Format Plugin when handling PNG files. This can be exploited to cause a stack-based buffer overflow via a specially crafted PNG file.

Successful exploitation allows execution of arbitrary code.

The vulnerability is confirmed in Adobe Photoshop CS2 and Adobe Photoshop Elements (Editor) version 5.0 for Windows and reportedly affects Adobe Photoshop CS3.

References:
http://milw0rm.com/exploits/3812

Cisco PIX and ASA Denial of Service and Security Bypass
"Denial of Service"

Some vulnerabilities have been reported in Cisco PIX and ASA, which can be exploited by malicious people to bypass certain security restrictions or cause a DoS (Denial of

Service).

1) An unspecified error exists when using the LDAP authentication mechanism, which can be exploited to bypass the authentication and gain access to the device or the network.

Successful exploitation requires that the device uses the Layer 2 Tunneling Protocol (L2TP) and is configured to use LDAP servers with another protocol other than PAP for authentication, or that the device offers remote management access (telnet, SSH, HTTP) and uses an LDAP AAA server for authentication.

2) An unspecified error when using VPN connections configured with password expiry can be exploited to cause a DoS.

Successful exploitation requires that the tunnel group is configured with password expiry. In order to exploit this in IPSec VPN connections, an attacker also needs to know the group name and group password.

3) A race condition within the processing of non-standard SSL sessions in the SSL VPN server of Cisco ASA appliances can be exploited to cause the device to reload.

Successful exploitation requires that clientless SSL is used.

4) An error within the DHCP relay agent when handling DHCPACK messages can be exploited to cause a DoS due to memory exhaustion by sending a large number of DHCP requests to a vulnerable device.

Successful exploitation requires that devices are configured to use the DHCP relay agent.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20070502-asa.shtml
http://www.cisco.com/warp/public/707/cisco-sr-20070502-pix.shtml

Word Viewer OCX ActiveX Control Buffer Overflow Vulnerabilities
"Execution of arbitrary code"

shinnai has discovered some vulnerabilities in Word Viewer OCX, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to boundary errors within the Word Viewer ActiveX control (WordViewer.ocx). These can be exploited to cause stack-based buffer overflows via overly long arguments passed to certain methods (e.g. "HttpDownloadFile()" or "OpenWebFile()").

Successful exploitation may allow execution of arbitrary code when a user visits a malicious website.

The vulnerabilities are confirmed in version 3.2.0.5. Other versions may also be affected.

References:
http://moaxb.blogspot.com/2007/05/moaxb-03-wordviewerocx-32-multiple_03.html

Trillian Information Leakage and Buffer Overflow Vulnerabilities
"Gain knowledge of sensitive information; Execution of arbitrary code"

Some vulnerabilities have been reported in Trillian, which can be exploited by malicious people to gain knowledge of sensitive information or compromise a user's system.

1) An error within the copy operation in an IRC message window (by highlighting the text) can be exploited to cause a heap-based buffer overflow via an overly long URL string consisting of UTF-8 characters.

Successful exploitation may allow execution of arbitrary code, but requires that a user is tricked into e.g. highlighting the malicious URL in an IRC message window.

2) An error within the IRC module can be exploited to cause a heap-based buffer overflow via an overly long, specially crafted message containing a font face HTML tag with the face attribute set to a long UTF-8 string.

Successful exploitation may allow execution of arbitrary code.

3) An error within the handling of CTCP PING messages containing UTF-8 characters can be exploited to make the client return a malformed response with no terminating newline character. This could allow the next line to be sent to the attacker instead of the server.

4) An error within the Rendezvous / XMPP (Extensible Messaging and Presence Protocol) messaging subsystem can be exploited to cause a heap-based buffer overflow via a specially crafted message sent to default port 5298/TCP.

Successful exploitation allows execution of arbitrary code.

The vulnerabilities are reported in version 3.1. Other versions may also be affected.

References:
http://blog.ceruleanstudios.com/?p=131
http://blog.ceruleanstudios.com/?p=129#more-129
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=522
http://dvlabs.tippingpoint.com/advisory/TPTI-07-06

ISC BIND "query_addsoa" Denial of Service
“Denial of Service”

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

The vulnerability is caused due to an error when invoking the "query_addsoa()" function. This can be exploited to cause the nameserver to exit by sending a specially crafted sequence of queries.

Successful exploitation requires that "recursion" is enabled.

The vulnerability is reported in BIND version 9.4.0, and BIND versions 9.5.0a1, 9.5.0a2, and 9.5.0a3.

References:
http://www.isc.org/sw/bind/bind-security.php

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