ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 24

June 22, 2007

Table of Contents

Product Focus

Sapphire Worm Scanner – The Sapphire Worm 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 Microsoft SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

This Week in Review

This week netVigilance Security Research has found 3 vulnerabilities in open source software WSPortal and Utopia News:

1 high risk, 1 medium risk and 1 low risk. The vulnerabilities include SQL Injection, XSS (Cross site Scripting) and Path Disclosure Vulnerabilities.

To see details and further information please see:
http://www.netvigilance.com/advisories

A secure internet - continued.The fear of Big Brother rumbles again. The things forming security.Iphone: Good or bad?

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

❖ A secure Internet requires a secure network protocol

Implementing -- and requiring -- stronger authentication and cryptography standards is the next step toward a new Internet
This is my third column on creating a more secure computing ecosystem. My first two columns summarized the larger ideas behind this project: It begins with secure hardware and moves on to secure booting, a secure OS, secure applications, and authenticated users, as well as the ability to track network packets from start to end. Supporters have so far outnumbered critics four to one (whatever that means in a nonrandom survey). Reader Michael Hartmann was among the many proponents of the solution. I like the way he captured the idea: “I think making the Internet more secure is really analogous to making any human society more secure. Anarchy is the easiest but riskiest course, and forming a government of laws is difficult but a necessary evil. Without some form of agreed-upon limits, there really is no method for fairly and effectively policing the miscreants. With a system of verification, we have the start of security, just like we have the start of some reasonable security with a judicial system and other safeguards.”

As a former mohawk-wearing punk rocker (I wish I was making that up), I loved anarchy as an ideal. But I noticed that all my punk friends still called the police when someone hit them or stole their property.

infoworld

Full Story :
http://www.infoworld.com/article/07/06/22/25OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/06/22/25OPsecadvise_1.html

❖ Big Brother is watching you... and he's a computer

The threat of cameras combined with artificial intelligence
Privacy activists have been lamenting increasing surveillance by cameras and warn of abuse by authorities who have access to them. But two additional trends portend a disturbing new direction.

The first trend: Cameras are increasingly monitoring noncriminals engaged in technically legal behavior. The second trend: Special new artificial intelligence software is processing video feeds to look for unacceptable behavior.

The machines are watching us, and they are making judgments about what we do.

Another way of looking at these colliding trends is that we are beginning to offload the human capacity for ethics, morality and good citizenship to computer systems. At the very least, these systems are replacing the traditional role of the nosy neighbor.

computerworld

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

myName=security&articleId=9025469&taxonomyId=17&intsrc=kc_feat

- **Perfectly Formed Internet Security**

Every company needs to build an IT security fortress to protect themselves and their data against Internet threats. The problem is, where do you put the strongest defences? How big do the defences need to be? And how do you marshal and manage resources to keep those defences strong?

With serious threats emerging both from within and without, all businesses have similar fundamental security concerns. All have a requirement to block spam, prevent Web and email-borne malware reaching the network and ensure that Web and e-mail usage is not creating security or productivity issues. However it's hard to know exactly which security measures to apply, and where, to make your budgets go furthest. That's true for any business, of any size.

bios

Full Story :
http://www.biosmagazine.co.uk/op.php?id=635

- **iPhone Has Neither Security nor Relevance**

Apple's upcoming iPhone: It's a "security nightmare," it will "turn your security team into zombies," and Apple is possibly "using the Windows Safari Beta Test to stamp out iPhone security holes."

Or, then again, depending on which iPhone watcher you're paying attention to, the iPhone security is irrelevant compared with "insecure wireless access points, tape backups disappearing, wrapping your newspapers in customers' personal financial information, and stolen laptops."
The iPhone won't go on sale until June 29. Up until now, and probably until it hits retail shelves, Apple has given next to nil information regarding the security features its first smart phone will have, making security analysis little better than conjecture. The few pieces of security background analysts have to go on include these tidbits: 1) The iPhone will run on Mac OS X and 2) the iPhone will run Apple's Safari browser.

eweek

Full Story :
http://www.eweek.com/article2/0,1895,2149610,00.asp

New Vulnerabilities Tested in SecureScout

- **16041 Trillian Information disclosure via long CTCP PING messages that contain UTF-8 characters (Remote File Checking)**

Cerulean Studios Trillian Pro before 3.1.5.1 allows remote attackers to obtain potentially sensitive information via long CTCP PING messages that contain UTF-8 characters, which generates a malformed response that is not truncated by a newline, which can cause portions of a server message to be sent to the attacker.

The vulnerability is reported fixed in version 3.1.5.1.

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

References:

Original advisory:
# IDEFENSE:20070501 Cerulean Studios Trillian Multiple IRC Vulnerabilities
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=522

Other references:
# CONFIRM: http://blog.ceruleanstudios.com/?p=131
# BID:23730
# URL:http://www.securityfocus.com/bid/23730
# FRSIRT:ADV-2007-1596
# URL:http://www.frsirt.com/english/advisories/2007/1596
# SECTRACK:1017982
# URL:http://www.securitytracker.com/id?1017982
# SECUNIA:25086
# URL:http://secunia.com/advisories/25086
# XF:trillian-ctcpping-information-disclosure(33983)
# URL:http://xforce.iss.net/xforce/xfdb/33983
# URL:http://xforce.iss.net/xforce/xfdb/33986

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

CVE Reference: CVE-2007-2479

❖ 15626 Trillian Multiple heap-based buffer overflows in the IRC component (Remote File Checking)

Multiple heap-based buffer overflows in the IRC component in Cerulean Studios Trillian Pro before 3.1.5.1 allow remote attackers to corrupt memory and possibly execute arbitrary code via (1) a URL with a long UTF-8 string, which triggers the overflow when the user highlights it, or (2) a font HTML tag with a face attribute containing a long UTF-8 string.

The vulnerability is reported fixed in version 3.1.5.1.

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

References:

Original advisory:
# IDEFENSE:20070501 Cerulean Studios Trillian Multiple IRC Vulnerabilities
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=522

Other references:
# CONFIRM: http://blog.ceruleanstudios.com/?p=131

# BID:23730
# URL:http://www.securityfocus.com/bid/23730
# FRSIRT:ADV-2007-1596
# URL:http://www.frsirt.com/english/advisories/2007/1596
# SECTRACK:1017982
# URL:http://www.securitytracker.com/id?1017982
# SECUNIA:25086
# URL:http://secunia.com/advisories/25086
# XF:trillian-fontface-bo(33986)
# URL:http://xforce.iss.net/xforce/xfdb/33986
# XF:trillian-urlhighlight-bo(33985)
# URL:http://xforce.iss.net/xforce/xfdb/33985

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

CVE Reference: CVE-2007-2478

❖ 15623 Trillian UTF-8 Word Wrap Buffer Overflow Vulnerability (Remote File Checking)

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

The vulnerability is caused due to a boundary error when word-wrapping UTF-8 strings in a message window. This can be exploited to cause a heap-based buffer overflow when a user views an overly long, specially crafted message using e.g. the MSN protocol.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported fixed in version 3.1.6.0.

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

References:

Original advisory:
# IDEFENSE:20070618 Cerulean Studios Trillian UTF-8 Word Wrap Heap Overflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=545

Other references:
# CONFIRM: http://blog.ceruleanstudios.com/?p=150
# BID:24523
# URL:http://www.securityfocus.com/bid/24523
# FRSIRT:ADV-2007-2246
# URL:http://www.frsirt.com/english/advisories/2007/2246
# SECUNIA:25736
# URL:http://secunia.com/advisories/25736

Product Homepage:

http://www.ceruleanstudios.com/

CVE Reference: CVE-2007-3305

❖ 14054 Samba smbd logic error in the SID/Name translation functionality, privileges escalation Vulnerability

A vulnerability has been reported in Samba, which can be exploited by malicious users to perform certain actions with escalated privileges.

An error in smbd when translating SIDs to and from names can be exploited to issue SMB/CIFS protocol operations as the root user.

Successful exploitation requires a valid user session.

The security issue has been fixed in version 3.0.25.

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

References:

Initial advisory:
# BUGTRAQ:20070513 [SAMBA-SECURITY] CVE-2007-2444: Local SID/Name Translation Failure Can Result in User Privilege Elevation
http://www.securityfocus.com/archive/1/archive/1/468548/100/0/threaded
# BUGTRAQ:20070515 FLEA-2007-0017-1: samba
http://www.securityfocus.com/archive/1/archive/1/468670/100/0/threaded

Product Page:
http://www.samba.org

CVE Reference: CVE-2007-2444

❖ 14052 Samba arbitrary shell commands execution via a specially crafted MS-RPC call

An input validation error when updating a user's password can be exploited to inject and execute arbitrary shell commands via a specially crafted MS-RPC call.

Successful exploitation of this vulnerability requires that the "username map script" option is set in smb.conf, which is not the default setting. In addition, to successfully exploit this vulnerability via remote printer and file share management, an attacker requires a valid user session.

The security issue has been fixed in version 3.0.25.

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

References:

Initial advisory:
# IDEFENSE:20070514 Samba SAMR Change Password Remote Command Injection Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534
# BUGTRAQ:20070513 [SAMBA-SECURITY] CVE-2007-2447: Remote Command Injection Vulnerability
http://www.securityfocus.com/archive/1/archive/1/468565/100/0/threaded
# BUGTRAQ:20070515 FLEA-2007-0017-1: samba
http://www.securityfocus.com/archive/1/archive/1/468670/100/0/threaded

Product Page:
http://www.samba.org

CVE Reference: CVE-2007-2447

❖ 16529 Vulnerability in Windows Vista Could Allow Information Disclosure (MS07-032/931213) (Remote File Checking)

There is an information disclosure vulnerability in Windows Vista that could allow non-privileged users to access local user information data stores including administrative passwords contained within the registry and local file system. The vulnerability could allow a local attacker to have access to user account data that could then be used in an attempt to gain full access to the affected system.

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

References:

Original advisory:
* MS:MS07-032
http://www.microsoft.com/technet/security/bulletin/ms07-032.mspx

Other references:
# CERT:TA07-163A
# URL:http://www.us-cert.gov/cas/techalerts/TA07-163A.html
# BID:24411
# URL:http://www.securityfocus.com/bid/24411
# FRSIRT:ADV-2007-2152
# URL:http://www.frsirt.com/english/advisories/2007/2152
# SECTRACK:1018225
# URL:http://www.securitytracker.com/id?1018225
# SECUNIA:25623
# URL:http://secunia.com/advisories/25623

CVE Reference: CVE-2007-2229

❖ 16528 Microsoft Visio Document Packaging Vulnerability (MS07-030/927051) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Visio as a result of the way it incorrectly handles the parsing of packed objects within the Visio file format. An attacker could exploit this vulnerability by constructing a malicious Visio (.VSD, VSS, or .VST) file that could potentially allow remote code execution if a user visited a malicious Web site or opened a specially crafted Visio attachment included in an e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
* MS:MS07-030
http://www.microsoft.com/technet/security/bulletin/ms07-030.mspx

Other references:
# CERT:TA07-163A
# URL:http://www.us-cert.gov/cas/techalerts/TA07-163A.html
# BID:24384
# URL:http://www.securityfocus.com/bid/24384
# FRSIRT:ADV-2007-2150
# URL:http://www.frsirt.com/english/advisories/2007/2150
# SECTRACK:1018227
# URL:http://www.securitytracker.com/id?1018227
# SECUNIA:25619
# URL:http://secunia.com/advisories/25619

CVE Reference: CVE-2007-0936

❖ 16527 Microsoft Visio Version Number Memory Corruption Vulnerability (MS07-030/927051) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Visio handles a specially crafted version number in a Visio (.VSD, VSS, or .VST) file. An attacker could exploit this vulnerability when Visio does not correctly validate the version number field when processing the contents of a file. Such a specially crafted file might be included as an e-mail attachment, or hosted on a malicious or compromised Web site.

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

References:

Original advisory:
* MS:MS07-030
http://www.microsoft.com/technet/security/bulletin/ms07-030.mspx

Other references:
# CERT:TA07-163A
# URL:http://www.us-cert.gov/cas/techalerts/TA07-163A.html
# BID:24349
# URL:http://www.securityfocus.com/bid/24349
# FRSIRT:ADV-2007-2150
# URL:http://www.frsirt.com/english/advisories/2007/2150
# SECTRACK:1018227

# URL:http://www.securitytracker.com/id?1018227
# SECUNIA:25619
# URL:http://secunia.com/advisories/25619
# XF:visio-version-code-execution(34607)
# URL:http://xforce.iss.net/xforce/xfdb/34607

CVE Reference: CVE-2007-0934

❖ 16526 Vulnerability in Win 32 API Could Allow Remote Code Execution (MS07-035/935839) (Remote File Checking)

A remote code execution vulnerability exists in the way that the Win32 API validates parameters. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
* MS:MS07-035
http://www.microsoft.com/technet/security/bulletin/ms07-035.mspx

Other references:
# CERT:TA07-163A
# URL:http://www.us-cert.gov/cas/techalerts/TA07-163A.html
# CERT-VN:VU#457281
# URL:http://www.kb.cert.org/vuls/id/457281
# BID:24370
# URL:http://www.securityfocus.com/bid/24370
# FRSIRT:ADV-2007-2155
# URL:http://www.frsirt.com/english/advisories/2007/2155
# SECTRACK:1018230
# URL:http://www.securitytracker.com/id?1018230
# SECUNIA:25640
# URL:http://secunia.com/advisories/25640

CVE Reference: CVE-2007-2219

❖ 16515 Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (MS07-031/935840) (Remote File Checking)

A remote code execution vulnerability exists in the way that Windows Schannel on a client machine validates server-sent digital signatures. An attacker could host a specially crafted Web site that is designed to exploit these vulnerabilities through an Internet Web browser and then convince a user to view the Web site. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or in an Instant Messenger message that takes users to the attacker's Web site.

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

References:

Original advisory:
* MS:MS07-031
http://www.microsoft.com/technet/security/bulletin/ms07-031.mspx

CVE Reference: CVE-2007-2218

New Vulnerabilities found this Week

Trillian UTF-8 Word Wrap Buffer Overflow Vulnerability

"Execution of arbitrary code"

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

The vulnerability is caused due to a boundary error when word-wrapping UTF-8 strings in a message window. This can be exploited to cause a heap-based buffer overflow when a user views an overly long, specially crafted message using e.g. the MSN protocol.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in version 3.1.5.1. Other versions may also be affected.

References:
http://blog.ceruleanstudios.com/?p=150
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=545
http://www.kb.cert.org/vuls/id/187033

Apple Mac OS X IPv6 Type 0 Route Headers Denial of Service

"Denial of Service"

A security issue has been reported in Apple Mac OS X, which can be exploited by malicious people to cause a DoS (Denial of Service).

The security issue is caused due to an error within the processing of packets with IPv6 type 0 route headers. This can be exploited to cause a DoS due to high network traffic by sending specially crafted IPv6 packets to vulnerable systems.

The security issue is reported in versions prior to Mac OS X 10.4.10.

NOTE: The security issue does not affect systems prior to Mac OS X 10.4.

References:
http://docs.info.apple.com/article.html?artnum=305712
http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf

Apple TV UPnP IGD Buffer Overflow Vulnerability

“Denial of Service; Execution of arbitrary code”

A vulnerability has been reported in Apple TV, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable device.

The vulnerability is caused due to a boundary error within the UPnP IGD (Internet Gateway Device Standardized Device Control Protocol) implementation and can be exploited to cause a buffer overflow.

Successful exploitation may allow execution of arbitrary code.

References:
http://docs.info.apple.com/article.html?artnum=305631

Sun StarOffice Office Suite RTF File and FreeType Font Parsing Vulnerabilities

“Code execution”

Sun has acknowledged two vulnerabilities in Sun StarOffice, which can be exploited by malicious people to compromise a user's system.

1) An error exists when parsing the "prdata" tag in RTF files where the first token is smaller that the second one. This can be exploited to cause a heap-based buffer overflow by e.g. tricking a user into opening a specially crafted RTF files.

2) A vulnerability is caused due to the use of a vulnerable copy of the FreeType library, which can be exploited to cause a heap based buffer overflow by e.g. tricking a user into opening a specially crafted document.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102967-1
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102917-1

Linux Kernel "compat_sys_mount()" Denial of Service Security Issue

“Denial of Service”

A security issue has been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The security issue is caused due to a NULL pointer dereference error in the "compat_sys_mount()" function in fs/compat.c, which can be exploited to crash a vulnerable system by mounting an smbfs file system in compatibility mode.

References:
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff_plain;h=822191a2fa1584a29c3224ab328507adcaeac1ab

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