netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 20

May 19, 2006

Table of Contents

Product Focus

Sasser Worm Scanner – The Sasser 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 SSL Vulnerablility (MS04-011) that used by the Sasser Worm to infect machines.

This Week in Review

AntiSpam company killed by Spammers; Virus uses file-sharing to leak powerplant info; U.K Gov wants Crypto Keys,

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

- **Security Feature Could Irk Vista Users**

Beta 2 testers can expect to encounter an obtrusive security feature, called User Account Control (UAC). Designed to prevent intruders from performing harmful tasks, the feature grays out the computer screen, then prods you to confirm that you really want to

do certain functions.

An annoying surprise awaits 2 million consumers expected to enthusiastically step forward in the next few weeks to help Microsoft test its new Windows Vista PC operating system.

Volunteers will test Vista Beta 2, a near-final version of the much-hyped upgrade of Windows. The testing is the last step leading up to Vista's broad consumer release, scheduled for January.

CIO Today

Full Story :
http://www.cio-today.com/story.xhtml?story_id=103003JTXEER

❖ Virus leaks power station security info

Sensitive security information about a Japanese thermoelectric power plant run by the Chubu Electric Power Company has been leaked onto the internet following a virus infection, according to media reports.

The virus, which has not been named in the reports, is said to have disseminated documents regarding the plant's security arrangements, names and addresses of its security personnel and other confidential information, via the popular Share file-sharing program.

The incident occurred after a 40 year-old security employee at Chubu Electric installed Share on his computer in March.

IT Week

Full Story :
http://www.itweek.co.uk/vnunet/news/2156317/virus-leaks-power-station-info

❖ Blue Security Shutters After Brutal Spam Attack

Blue Security, an Internet security firm that tried to fight spam with spam, has shut down after a prolonged denial-of-service launched by the spammers it hoped to put out of business.

The Israel-based company tried to use the tactics of spammers against it, using a system that automatically sent messages back to them, operating on the theory that doing so

would overload the servers of the original spammers and put them out of commission -- at least, temporarily.
E-Commerce News

Full Story :

http://www.ecommercetimes.com/rsstory/50609.html

Technical details :

http://www.renesys.com/blog/2006/05/the_bluesecurity_fiasco_dont_m.shtml

- **Vista 'underwhelming' on Security says Yankee**

The British government is preparing to give its police the authority to force organizations and individuals to disclose encryption keys, a move that has outraged some security and civil-rights experts.

The legislation that gives the police such authority is contained within Part 3 of the Regulation of Investigatory Powers Act. The RIP Act, also known as RIPA, was introduced in 2000, but the government has held back from bringing Part 3 into effect. Now, more than five years after the original act was passed, the Home Office is seeking to exercise the powers within Part 3.

CNET News

Full Story :

http://news.com.com/British%20legislation%20to%20enforce%20encryption%20key%20disclosure/2100-7348_3-6073654.html?tag=nefd.top

New Vulnerabilities Tested in SecureScout

- **16238 Linux Kernel SCTP deadlock, Denial of Service Vulnerability**

An deadlock error within the handling of the receive buffer in SCTP can be exploited to cause a DoS via a large number of small messages sent to a receiver application that causes it to run of receive buffer space.

The vulnerability has been reported in versions prior to 2.6.16.15.

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

References:

Original advisory:
http://git.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=7c3ceb4fb9667f34f1599a062efecf4cdc4a4ce5

Other references:
http://secunia.com/advisories/19990/

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-2275

❖ 16239 Linux Kernel "lease_init()" Denial of Service Vulnerability

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

The vulnerability is caused due to a error within the "lease_init()" function in "fs/locks.c". This causes it to free memory that may not have been allocated using the "locks_alloc_lock()" function. This may cause the kernel to crash when the "fcntl_setlease()" function is called.

The vulnerability has been reported in versions prior to 2.6.16.16.

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

References:

Original advisory:
http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=commit;h=1f0e637c94a9b041833947c79110d6c02fff8618

Other references:
* CONFIRM:http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.16
* CONFIRM:http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=blobdiff;h=aa7f66091823dde953e15895dc427615701c39c7;hp=e75ac392a313f3fad823bf2e46a03f29701e3e34;hb=1f0e637c94a9b041833947c79110d6c02fff8618;f=fs/locks.c
* BID:17943
* URL:http://www.securityfocus.com/bid/17943
* FRSIRT:ADV-2006-1767
* URL:http://www.frsirt.com/english/advisories/2006/1767
* SECUNIA:20083
* URL:http://secunia.com/advisories/20083

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1860

❖ 16240 QuickTime Code Execution Vulnerability within the processing of JPEG images (Remote File Checking)

A vulnerability has been reported in QuickTime, which can be exploited by malicious people to execute arbitrary code.

An integer overflow error within the processing of JPEG images can be exploited via a specially crafted JPEG image to crash the application and potentially execute

arbitrary code.

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

References:

References:
Original Advisory:
* APPLE:APPLE-SA-2006-05-11
http://lists.apple.com/archives/security-announce/2006/May/msg00002.html

Other references:
* CERT-VN:VU#289705
* URL:http://www.kb.cert.org/vuls/id/289705
* BID:17953
* URL:http://www.securityfocus.com/bid/17953
* SECTRACK:1016067
* URL:http://securitytracker.com/id?1016067
* SECUNIA:20069
* URL:http://secunia.com/advisories/20069

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

CVE Reference: CVE-2006-1458

❖ 16241 QuickTime Code Execution Vulnerability within the processing of QuickTime movies (Remote File Checking)

A vulnerability has been reported in QuickTime, which can be exploited by malicious people to execute arbitrary code.

An integer overflow and boundary error within the processing of QuickTime movies can be exploited via a specially crafted QuickTime movie to crash the application and potentially execute arbitrary code.
Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
* APPLE:APPLE-SA-2006-05-11
http://lists.apple.com/archives/security-announce/2006/May/msg00002.html

Other references:
* BUGTRAQ:20060512 Apple QuickDraw/QuickTime Multiple Vulnerabilities
* URL:http://www.securityfocus.com/archive/1/archive/1/433831/100/0/threaded
* BID:17953
* URL:http://www.securityfocus.com/bid/17953
* SECTRACK:1016067
* URL:http://securitytracker.com/id?1016067
* SECUNIA:20069
* URL:http://secunia.com/advisories/20069

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

CVE Reference: CVE-2006-1459

❖ 16242 QuickTime Code Execution Vulnerability within the processing of Flash movies (Remote File Checking)

A vulnerability has been reported in QuickTime, which can be exploited by malicious people to execute arbitrary code.

A boundary error within the processing of Flash movies can be exploited via a specially crafted Flash movie to crash the application and potentially execute arbitrary code.
Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original Advisory:
* APPLE:APPLE-SA-2006-05-11
http://lists.apple.com/archives/security-announce/2006/May/msg00002.html

Other references:
* BUGTRAQ:20060512 Apple QuickDraw/QuickTime Multiple Vulnerabilities
* URL:http://www.securityfocus.com/archive/1/archive/1/433831/100/0/threaded
* BID:17953
* URL:http://www.securityfocus.com/bid/17953
* SECTRACK:1016067
* URL:http://securitytracker.com/id?1016067
* SECUNIA:20069
* URL:http://secunia.com/advisories/20069

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

CVE Reference: CVE-2006-1461

❖ 16243 QuickTime Code Execution Vulnerability within the processing of H.264 movies (Remote File Checking)

A vulnerability has been reported in QuickTime, which can be exploited by malicious people to execute arbitrary code.

An integer overflow and boundary error within the processing of H.264 movies can be exploited via a specially crafted H.264 movie to crash the application and potentially execute arbitrary code.

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

References:

Original Advisory:

* APPLE:APPLE-SA-2006-05-11
http://lists.apple.com/archives/security-announce/2006/May/msg00002.html

Other references:
* BUGTRAQ:20060512 Apple QuickDraw/QuickTime Multiple Vulnerabilities
* URL:http://www.securityfocus.com/archive/1/archive/1/433831/100/0/threaded
* BID:17953
* URL:http://www.securityfocus.com/bid/17953
* SECTRACK:1016067
* URL:http://securitytracker.com/id?1016067
* SECUNIA:20069
* URL:http://secunia.com/advisories/20069

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

CVE Reference: CVE-2006-1462

❖ 16244 QuickTime Code Execution Vulnerability within the processing of MPEG4 movies (Remote File Checking)

A vulnerability has been reported in QuickTime, which can be exploited by malicious people to execute arbitrary code.

A boundary error within the processing of MPEG4 movies can be exploited via a specially crafted MPEG4 movie to crash the application and potentially execute arbitrary code.

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

References:

Original Advisory:
* APPLE:APPLE-SA-2006-05-11
http://lists.apple.com/archives/security-announce/2006/May/msg00002.html

Other references:
* BUGTRAQ:20060512 Apple QuickDraw/QuickTime Multiple Vulnerabilities
* URL:http://www.securityfocus.com/archive/1/archive/1/433831/100/0/threaded
* BID:17953
* URL:http://www.securityfocus.com/bid/17953
* SECTRACK:1016067
* URL:http://securitytracker.com/id?1016067
* SECUNIA:20069
* URL:http://secunia.com/advisories/20069

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

CVE Reference: CVE-2006-1464

❖ 16245 QuickTime Code Execution Vulnerability within the processing of

FlashPix images (Remote File Checking)

A vulnerability has been reported in QuickTime, which can be exploited by malicious people to execute arbitrary code.

An integer overflow error within the processing of FlashPix images (".fpx") can be exploited via a specially crafted FlashPix image with an overly large value in the field specifying the number of data blocks in the file. This can be exploited to cause a heap-based buffer overflow and allows execution of arbitrary code.

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

References:

Original Advisory:
* APPLE:APPLE-SA-2006-05-11
http://lists.apple.com/archives/security-announce/2006/May/msg00002.html

Other references:
* MISC:http://www.eeye.com/html/research/upcoming/20060307b.html
* BUGTRAQ:20060512 Apple QuickDraw/QuickTime Multiple Vulnerabilities
* URL:http://lists.apple.com/archives/security-announce/2006/May/msg00002.html
* BID:17074
* URL:http://www.securityfocus.com/bid/17074
* SECTRACK:1016067
* URL:http://securitytracker.com/id?1016067
* SECUNIA:20069
* URL:http://secunia.com/advisories/20069

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

CVE Reference: CVE-2006-1249

❖ **16246 QuickTime Code Execution Vulnerability within the processing of AVI movies (Remote File Checking)**

A vulnerability has been reported in QuickTime, which can be exploited by malicious people to execute arbitrary code.

A boundary error within the processing of AVI movies can be exploited via a specially crafted AVI movie to crash the application and potentially execute arbitrary code.

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

References:

Original Advisory:
* APPLE:APPLE-SA-2006-05-11
http://lists.apple.com/archives/security-announce/2006/May/msg00002.html

Other references:
* BUGTRAQ:20060512 Apple QuickDraw/QuickTime Multiple Vulnerabilities

* URL:http://www.securityfocus.com/archive/1/archive/1/433831/100/0/threaded
* APPLE:APPLE-SA-2006-05-11
* URL:http://lists.apple.com/archives/security-announce/2006/May/msg00002.html
* BID:17953
* URL:http://www.securityfocus.com/bid/17953
* SECTRACK:1016067
* URL:http://securitytracker.com/id?1016067
* SECUNIA:20069
* URL:http://secunia.com/advisories/20069

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

CVE Reference: CVE-2006-1465

❖ 16247 QuickTime Code Execution Vulnerability within the processing of PICT images (Remote File Checking)

Two vulnerabilities have been reported in QuickTime, which can be exploited by malicious people to execute arbitrary code.

Two boundary errors within the processing of PICT images can be exploited to either cause a stack-based buffer overflow via a PICT image with specially crafted font information or a heap-based buffer overflow via a PICT image with specially crafted image data. This can be exploited to crash the application and potentially execute arbitrary code.

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

References:

References:
Original Advisory:
* APPLE:APPLE-SA-2006-05-11
http://lists.apple.com/archives/security-announce/2006/May/msg00002.html
http://lists.apple.com/archives/security-announce/2006/May/msg00003.html

Other references:
* BUGTRAQ:20060512 Apple QuickDraw/QuickTime Multiple Vulnerabilities
* URL:http://www.securityfocus.com/archive/1/archive/1/433831/100/0/threaded
* CERT:TA06-132A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-132A.html
* BID:17953
* URL:http://www.securityfocus.com/bid/17953
* SECTRACK:1016067
* URL:http://securitytracker.com/id?1016067
* SECUNIA:20069
* URL:http://secunia.com/advisories/20069
* SECUNIA:20077
* URL:http://secunia.com/advisories/20077

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

CVE Reference: CVE-2006-1453

New Vulnerabilities found this Week

QuickTime Multiple Code Execution Vulnerabilities

"Code Execution"

Multiple Code Execution vulnerabilities have been reported in QuickTime, which can be exploited by malicious people to compromise a user's system.

References:

http://docs.info.apple.com/article.html?artnum=303752

http://www.eeye.com/html/research/advisories/AD20060511.html

http://www.zerodayinitiative.com/advisories/ZDI-06-015.html

http://secway.org/advisory/AD20060512.txt

http://www.kb.cert.org/vuls/id/289705

http://www.kb.cert.org/vuls/id/570689

http://descriptions.securescout.com/tc/16240

http://descriptions.securescout.com/tc/16241

http://descriptions.securescout.com/tc/16242

http://descriptions.securescout.com/tc/16243

http://descriptions.securescout.com/tc/16244

http://descriptions.securescout.com/tc/16245

http://descriptions.securescout.com/tc/16246

http://descriptions.securescout.com/tc/16247

FreeFTPd SFTP Key Exchange Algorithm String Buffer Overflow

"Denial of Service"

A vulnerability has been reported in FreeFTPd, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

The vulnerability has been reported in version 1.0.10. Prior versions may also be affected.

References:

http://freeftpd.com/?ctt=changelog

Nagios Content-Length Integer Overflow Vulnerability

“Denial of Service”

A vulnerability has been reported in Nagios, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

The vulnerability is caused due to an integer overflow error within the handling of the "Content-Length" HTTP header. This can be exploited to cause a buffer overflow and may allow arbitrary code execute via a HTTP request with specially crafted value in the "Content-Length" HTTP header.

The vulnerability has been reported in the 1.x and 2.x code branches.

References:
http://www.nagios.org/development/changelog.php
http://www.nagios.org/development/changelog.php#1x_branch

phpMyAdmin "theme" and "db" Cross-Site Scripting Vulnerabilities

“Cross-site scripting”

Two vulnerabilities have been reported in phpMyAdmin, which can be exploited by malicious people to conduct cross-site scripting attacks.

1) Input passed to the "theme" parameter 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 vulnerability has been reported in versions prior to 2.8.0.4 for the 2.8.0 branch.

2) Input passed to the "db" parameter 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 vulnerability has been reported in some versions prior to 2.8.0.4.

References:
http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2006-2

Mac OS X Security Update Fixes Multiple Vulnerabilities
"Security Bypass; Exposure of sensitive information; DoS; System access"

Apple has issued a security update for Mac OS X, which fixes multiple vulnerabilities.

References:
http://docs.info.apple.com/article.html?artnum=303737
http://www.kb.cert.org/vuls/id/519473

RealVNC Password Authentication Bypass Vulnerability
"Bypass authentication"

Steve Wiseman has reported a vulnerability in RealVNC, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an error within the handling of VNC password authentication requests. This can be exploited to bypass authentication and allows access to the remote system without requiring knowledge of the VNC password.

The vulnerability has been reported in version 4.1.1. Other versions may also be affected.

Note: Version 4.0 is reportedly not affected.

References:
http://www.realvnc.com/products/free/4.1/release-notes.html
http://www.realvnc.com/products/personal/4.2/release-notes.html
http://www.realvnc.com/products/enterprise/4.2/release-notes.html
http://www.intelliadmin.com/blog/2006/05/security-flaw-in-realvnc-411.html
http://www.intelliadmin.com/blog/2006/05/vnc-flaw-proof-of-concept.html
http://www.kb.cert.org/vuls/id/117929

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