netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 22

June 2, 2006

Table of Contents

Product Focus

Task Scheduler Vulnerability Scanner – The Task Scheduler 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 Task Scheduler flaw (MS04-022).

This Week in Review

Cyber terrorist worries, password found to unlock Ransomed docs, Brits will not pursue Ransomware maker, Yahoo get in crossfire for collaborating with China

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

- **The new breed of cyber-terrorist**

According to cyber-security experts, the terror attacks of 11 September and 7 July could be seen as mere staging posts compared to the havoc and devastation that might be unleashed if terrorists turn their focus from the physical to the digital world.

Scott Borg, the director and chief economist of the US Cyber Consequences Unit (CCU), a Department of Homeland Security advisory group, believes that attacks on computer networks are poised to escalate to full-scale disasters that could bring down companies and kill people. He warns that intelligence "chatter" increasingly points to possible criminal or terrorist plans to destroy physical infrastructure, such as power grids. Al-Qa'ida, he stresses, is becoming capable of carrying out such attacks.

The Independent

Full Story :
http://news.independent.co.uk/world/science_technology/article622421.ece

- **Password found for Arhiveus MayAlert trojan**

The new Arhiveus-A Trojan (also known as MayAlert) scoops up files in innocent users' 'My Documents' folders and creates a file called EncryptedFiles.als. When users try to access their documents they are directed to a file containing instructions on how to recover the data. The instructions begin:

'INSTRUCTIONS HOW TO GET YOUR FILES BACK READ CAREFULLY. IF YOU DO NOT UNDERSTAND - READ AGAIN.
This is the automated report generated by auto archiving software.

'Your computer caught our software while browsing illegal porn pages, all your documents, text files, databases in the folder
My Documents was archived with long password.

'You can not guess the password for your archived files - password length is more than 30 symbols that makes all password
recovery programs fail to bruteforce it (guess password by trying all possible combinations).

SecurityPark.net

Full Story :
http://www.securitypark.co.uk/article.asp?articleid=25403&CategoryID=1

- **Police will not pursue ransom hackers**

After a Manchester woman was held to ransom by hackers, experts and senior police officers have voiced concern that such cases are falling between the cracks

Greater Manchester Police (GMP) will not be pursuing the criminals who used a Trojan horse program to lock a Manchester woman's files and demanded a ransom to release them.

The malicious Archiveus program was unintentionally downloaded by Helen Barrow of Rochdale, who found it locked her files into a 30-character password-protected folder. A ransom note instructed her to avoid going to the police, and buy pharmaceutical products online to gain the password to release her files.

Barrow did not pay, and managed to recover some data. The police, however, will not be investigating the crime.

ZDNet UK

Full Story :

http://news.zdnet.co.uk/internet/0,39020369,39272579,00.htm

- **Yahoo Defends China Cooperation**

Yahoo's Terry Semel faced tough questions from Walt Mossberg — and the audience — over the search company's decision to comply with requests for user data from the Chinese government, which has used the information to pursue dissidents.

"I continue to be pissed off, outraged, and feel very very bad about it," Mr. Semel said. "But you have to follow the laws of the country you're in."

Mr. Semel went on: "I don't think any one company is going to change a country, and I dont think any one industry is going to change a country. "

One attendee asked Mr. Semel if Yahoo would have cooperated with Nazi Germany the same way it has with China. His response: "Yahoo has a basic obligation not to have a point of view on basic content, and to present content ... and aggregate things and to allow people to make their own choices. I don't know how I would have felt then." He added, "I don't feel good about what's happening in China today. I don't feel good about some of the things that happen in our own country."

The Wall Street Journal

Full Story :

http://blogs.wsj.com/dnotebook/2006/05/31/yahoo-defends-china-cooperation/

New Vulnerabilities Tested in SecureScout

- **14714 Mozilla Firefox error in the "InstallTrigger.install()" method to cause a memory corruption Vulnerability (Remote File Checking)**

A vulnerability has been reported in Firefox.

An error in the "InstallTrigger.install()" method can be exploited to cause a memory corruption.

The vulnerability has been reported in version 1.0.7 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-11.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-1790

- **14715 Mozilla Firefox secure lock icon spoofing Vulnerability (Remote File Checking)**

A vulnerability has been reported in Firefox.

An unspecified error can be exploited to spoof the secure lock icon and the address bar by changing the location of a pop-up window in certain situations.

Successful exploitation requires that the "Entering secure site" dialog has been enabled (not enabled by default).

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-12.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-1740

❖ 14716 Mozilla Firefox "Save image as..." to trick users into downloading malicious files (Remote File Checking)

A vulnerability has been reported in Firefox.

It is possible to trick users into downloading malicious files via the "Save image as..." menu option.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-13.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-1736

❖ 14717 Mozilla Firefox "eval()" call JavaScript function creation Code Execution Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox.

A JavaScript function created via an "eval()" call associated with a method of an XBL binding may be compiled with incorrect privileges. This can be exploited to execute arbitrary code.

The vulnerability has been reported in version 1.0 and 1.5.

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

References:

Original Advisories:
http://www.mozilla.org/security/announce/2006/mfsa2006-14.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-1735

❖ 16258 Linux Kernel input validation error in SCTP when processing HB-ACK chunk to cause system to crash

A vulnerability has been reported in the Linux Kernel, which can be exploited by

malicious people to cause a DoS.

An input validation error in SCTP when processing a HB-ACK chunk with a specially-crafted parameter length can be exploited to cause out-of-bounds memory access. This can potentially cause the system to crash.

The vulnerability has been reported in versions prior to 2.6.16.17.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.17

Other references:
BID:18085
URL:http://www.securityfocus.com/bid/18085
FRSIRT:ADV-2006-1893
URL:http://www.frsirt.com/english/advisories/2006/1893
SECUNIA:20185
URL:http://secunia.com/advisories/20185

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1857

❖ 16259 Linux Kernel error in SCTP chunk length calculation to cause system to crash

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious people to cause a DoS.

An error in SCTP chunk length calculation during parameter processing can be exploited to cause out-of-bounds memory access. This can potentially cause the system to crash.

The vulnerability has been reported in versions prior to 2.6.16.17.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.17

Other references:
BID:18085
URL:http://www.securityfocus.com/bid/18085
FRSIRT:ADV-2006-1893
URL:http://www.frsirt.com/english/advisories/2006/1893
SECUNIA:20185

URL:http://secunia.com/advisories/20185

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1858

❖ 16260 Linux Kernel race condition in netfilter "do_add_counters()" function allows users to read kernel memory or cause the system to crash

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious local people to cause a DoS.

A race condition in the "do_add_counters()" function in netfilter can be exploited by local users to read kernel memory or cause the system to crash via a race condition that produces a size value that is different from the size of the allocated memory.

Successful exploitation requires that the user is granted CAP_NET_ADMIN rights.

The vulnerability has been reported in versions prior to 2.6.16.17.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.17
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=191698
http://bugs.gentoo.org/show_bug.cgi?id=133465

Other references:
MISC: http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=2722971cbe831117686039d5c334f2c0f560be13
FRSIRT:ADV-2006-1893
URL:http://www.frsirt.com/english/advisories/2006/1893
SECUNIA:20185
URL:http://secunia.com/advisories/20185

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-0039

❖ 16261 Linux Kernel SNMP NAT Helper Denial of Service Vulnerability

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

The vulnerability is caused due to some errors within the "snmp_trap_decode()" function when handling certain SNMP packets. This can be exploited to cause memory corruption due to incorrect freeing of memory, which can potentially cause

the system to crash.

Successful exploitation requires that the "ip_nat_snmp_basic" module is loaded and that traffic NAT is enabled on port 161 or 162.

The vulnerability has been reported in versions prior to 2.6.16.18.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.18
http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=commit;h=1db6b5a66e93ff125ab871d6b3f7363412cc87e8

Other references:
MANDRIVA:MDKSA-2006:087
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:087
BID:18081
URL:http://www.securityfocus.com/bid/18081
SECUNIA:20225
URL:http://secunia.com/advisories/20225
SECUNIA:20182
URL:http://secunia.com/advisories/20182

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-2444

❖ 16262 Linux Kernel SMP "/proc" Race Condition Denial of Service Vulnerability

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

The vulnerability is cause due to a memory corruption error in the "dentry_unused" list within the "prune_dcache()" function. This can be exploited to crash the kernel when running on SMP hardware by causing a race condition such that one or more tasks exit while another task is reading their /proc entries.

The vulnerability has been reported in versions 2.6.15 to 2.6.17.

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

References:

Original advisory:
MLIST:[linux-kernel] 20060526 PROBLEM: /proc (procfs) task exit race condition causes a kernelcrash
http://marc.theaimsgroup.com/?l=linux-kernel&m=114860432801543&w=2

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-2629

❖ 17294 PHP "curl_init()" Safe Mode Bypass Vulnerability

Maksymilian Arciemowicz has discovered a vulnerability in PHP, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an error in the handling of null byte characters in the "curl_init()" PHP function in the curl extension. This can be exploited to bypass the safe mode protection and access other users' files located in the same directory as the running script.

Successful exploitation requires that the curl extension is installed and enabled.

The vulnerability has been confirmed in versions 5.0.5 and 5.1.4, and has also been reported in version 4.4.2. Other versions may also be affected.

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

References:

Original Advisory:
http://securityreason.com/achievement_securityalert/39

Other references:
* BUGTRAQ:20060526 cURL Safe Mode Bypass PHP 4.4.2 and 5.1.4
* URL:http://www.securityfocus.com/archive/1/archive/1/435194/100/0/threaded
* BID:18116
* URL:http://www.securityfocus.com/bid/18116

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-2563

New Vulnerabilities found this Week

F-Secure Products Web Console Buffer Overflow Vulnerability

"Allow execution of arbitrary code"

A vulnerability has been reported in F-Secure Anti-Virus for Microsoft Exchange and F-Secure Internet Gatekeeper, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified boundary error within the web console prior to authentication and can be exploited to cause a buffer overflow.

Successful exploitation crashes the web console process and may potentially allow execution of arbitrary code.

References:
http://www.f-secure.com/security/fsc-2006-3.shtml

FreeBSD SMBFS chroot Directory Traversal Vulnerability
"Bypass chroot restrictions"

A vulnerability has been reported in FreeBSD, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an input validation error in the SMBFS mounted file system and can be exploited to bypass chroot restrictions via the "..\" directory traversal sequence.

References:
http://security.freebsd.org/advisories/FreeBSD-SA-06:16.smbfs.asc

FreeBSD ypserv Inoperative Access Controls Security Issue
"Bypass Access Controls Security"

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

The problem is caused due to an error in ypserv as the "securenets" mechanism for restricting access to NIS maps is disabled.

References:
http://security.freebsd.org/advisories/FreeBSD-SA-06:15.ypserv.asc

Linux Kernel SMP "/proc" Race Condition Denial of Service

“Denial of Service”

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

The vulnerability is cause due to a memory corruption error in the "dentry_unused" list within the "prune_dcache()" function. This can be exploited to crash the kernel when running on SMP hardware by causing a race condition such that one or more tasks exit while another task is reading their /proc entries.

The vulnerability has been reported in versions 2.6.15 through 2.6.17. Other versions may also be affected.

References:
http://marc.theaimsgroup.com/?l=linux-kernel&m=114860432801543&w=2

PHP "curl_init()" Safe Mode Bypass Weakness

“Bypass the safe mode protection; access other users' files”

Maksymilian Arciemowicz has discovered a vulnerability in PHP, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an error in the handling of null byte characters in the "curl_init()" PHP function in the curl extension. This can be exploited to bypass the safe mode protection and access other users' files located in the same directory as the running script.

Successful exploitation requires that the curl extension is installed and enabled.

The vulnerability has been confirmed in versions 5.0.5 and 5.1.4, and has also been reported in version 4.4.2. Other versions may also be affected.

References:
http://securityreason.com/achievement_securityalert/39

Symantec Client Security / AntiVirus Unspecified Code Execution
"Execution of arbitrary code"

eEye Digital Security has reported a vulnerability in Symantec Client Security and Symantec AntiVirus Corporate Edition, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified boundary error and can be exploited to cause a stack-based buffer overflow.

Successful exploitation allows execution of arbitrary code with SYSTEM privileges.

References:
http://securityresponse.symantec.com/avcenter/security/Content/2006.05.25.html
http://www.eeye.com/html/research/upcoming/20060524.html

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