netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 35

September 1, 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

New bad IP-list service on its way. Software developers: Hacker awareness necessary on all levels. Phishing on the rise and turning very sophisticate – serious attacks are happening.

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

- **Datanet Security announced that the long awaited Trial offer is now available**

The Datanet Security Group announced today that the Trial offer of the Bad IP-ID Block List has been readied. The Bad IP-ID Block List is a dynamic honey-net collection of IP addresses sending malicious and undesirable electronic mail messages, including spam, spyware, phishing and zombie IP's. The CDIR pre-formatted list is dispatched per electronic mail.

The users are diversified; government entities, private and public companies as well as organizations and non-profits. Many Fortune-1000 enterprises have it as a standard pre-configured blacklist for their large corporate networks. Some deploy the list in compacted format within their ingress routing structure as an access control list (ACL). Others have it installed in their professional intrusion prevention and firewall systems.

IT Observer

Full Story :
http://www.it-observer.com/press.php?id=2635

- **How to thwart the attempts of attackers who try to gain knowledge of your application through its error handling messages**

When an application error occurs, whether due to user input or an internal function, we as conscientious developers want to present an error message that will help the end user correct the problem. However, it is possible to be too helpful with your error handling approach. By providing overly detailed application error messages to your users, you can actually be opening your site to hackers.

Hackers spend the majority of their time performing reconnaissance on a site, slowly gathering multiple pieces of information to determine how a site is vulnerable. Sometimes, it is a seemingly innocuous piece of information in an application error message that provides an attacker with the last piece of the puzzle necessary for him to launch a devastating attack.

SecurityPark.net

Full Story :
http://www.securitypark.co.uk/article.asp?articleid=25746&CategoryID=1

- **Experts warn of devious phishing attacks**

Phishing attacks will use more sophisticated social engineering, targeting consumers for financial and identity theft and businesses for intellectual property theft.

This is the main conclusion of the August 2006 global malware report released today by security firm MessageLabs.

The days of crude phishing emails which consumers have learned to spot are coming to a close, warns the report.

Cyber-criminals are now developing personalised approaches that ape legitimate businesses' customer relationship management techniques, or 'victim relationship management'.

vunet

Full Story :
http://www.vnunet.com/vnunet/news/2163387/phishing-sophisticated

- **Phishing expedition at heart of AT&T hacking**

When AT&T said in a press release this week that "unauthorized persons illegally hacked into a computer system and accessed personal data" from thousands of DSL customers, it wasn't telling the whole story.

Internal company documents show that the security breach was only the first step in a more elaborate scam that involved bogus e-mail being sent to AT&T customers that attempted to trick them into revealing additional info that could be used for widespread fraud or identity theft.

"We haven't seen anything like this before," acknowledged Walt Sharp, an AT&T spokesman.

San Fransisco Chronicle

Full Story :
http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2006/09/01/BUGVBKSUIE1.DTL&type=business

New Vulnerabilities Tested in SecureScout

- **16309 PHP "file_exists()", "imap_open()", and "imap_reopen()" functions Missing safe_mode and open_basedir verification Vulnerability**

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

Some vulnerabilities have been reported in PHP that can be exploited by malicious, local users to bypass certain security restrictions.

Missing safe_mode and open_basedir verification exists in the "file_exists()", "imap_open()", and "imap_reopen()" functions.

The vulnerabilities have been confirmed in versions 5.1.4 and 4.4.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.php.net/release_4_4_4.php
http://www.php.net/release_5_1_5.php

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

CVE Reference:

❖ 16310 PHP "str_repeat()" and "wordwrap()" functions boundary errors Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

Some vulnerabilities have been reported in PHP that can be exploited by malicious, local users to bypass certain security restrictions and execute arbitrary code.

Some unspecified boundary errors exists in the "str_repeat()" and "wordwrap()" functions on 64-bit systems.

The vulnerabilities have been confirmed in versions 5.1.4 and 4.4.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.php.net/release_4_4_4.php
http://www.php.net/release_5_1_5.php

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

CVE Reference:

❖ 16311 PHP cURL extension and realpath cache, open_basedir and safe_mode protection mechanisms bypass Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

Some vulnerabilities have been reported in PHP that can be exploited by malicious, local users to bypass certain security restrictions.

The open_basedir and safe_mode protection mechanisms can be bypassed via the cURL extension and the realpath cache.

The vulnerabilities have been confirmed in versions 5.1.4 and 4.4.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.php.net/release_4_4_4.php
http://www.php.net/release_5_1_5.php

Product Page:

http://www.php.net/

CVE Reference:

❖ 16312 PHP GD extension boundary error Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

A vulnerability has been reported in PHP that can be exploited by malicious, local users to bypass certain security restrictions or execute arbitrary code.

An unspecified boundary error exists in the GD extension when handling malformed GIF images.

The vulnerability has been confirmed in versions 5.1.4 and 4.4.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.php.net/release_4_4_4.php
http://www.php.net/release_5_1_5.php

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

CVE Reference:

❖ 16313 PHP "stripos()" function boundary error Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

A vulnerability has been reported in PHP that can be exploited by malicious, local users to bypass certain security restrictions or execute arbitrary code or disclose memory content.

A boundary error in the "stripos()" function can be exploited to cause an out-of-bounds memory read.

The vulnerability has been confirmed in versions 5.1.4 and 4.4.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.php.net/release_4_4_4.php
http://www.php.net/release_5_1_5.php

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

CVE Reference:

❖ 16314 PHP Incorrect memory_limit restrictions Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

A vulnerability has been reported in PHP that can be exploited by malicious, local users to execute arbitrary code.

Incorrect memory_limit restrictions exists on 64-bit systems.

The vulnerability has been confirmed in versions 5.1.4 and 4.4.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.php.net/release_4_4_4.php
http://www.php.net/release_5_1_5.php

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

CVE Reference:

❖ 16315 Linux Kernel SCTP Privilege Escalation Vulnerability

McAfee Avert Labs has reported a vulnerability in the Linux Kernel, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an error in the SCTP module within the "sctp_make_abort_user()" function and can be exploited to execute arbitrary code with escalated privileges.

The vulnerability has been reported in versions 2.4.23 through 2.4.32 and 2.6 up to and including 2.6.17.9. Other versions may also be affected.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.33.2

Other references:
BUGTRAQ:20060822 Linux Kernel SCTP Privilege Elevation Vulnerability
URL:http://www.securityfocus.com/archive/1/archive/1/444066/100/0/threaded
FULLDISC:20060822 Linux Kernel SCTP Privilege Elevation Vulnerability
URL:http://archives.neohapsis.com/archives/fulldisclosure/2006-08/0600.html
CONFIRM: http://kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.33.2
MANDRIVA:MDKSA-2006:150
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:150
MANDRIVA:MDKSA-2006:151
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:151
REDHAT:RHSA-2006:0617
URL:http://www.redhat.com/support/errata/RHSA-2006-0617.html
BID:19666
URL:http://www.securityfocus.com/bid/19666
SECUNIA:21605
URL:http://secunia.com/advisories/21605
SECUNIA:21576
URL:http://secunia.com/advisories/21576
SECUNIA:21614
URL:http://secunia.com/advisories/21614

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-3745

❖ 16316 Linux Kernel SG Driver Denial of Service Vulnerability

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

The vulnerability is caused due to an error in the SG driver and can be exploited to crash the system.

The vulnerability has been reported in versions lower than 2.4.33.1 or 2.6.13.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.33.1

Other references:
CONFIRM: https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=168791
CONFIRM: http://linux.bkbits.net:8080/linux-2.6/cset@43220081yu9ClBQNuqSSnW_9amW7iQ
MISC: http://marc.theaimsgroup.com/?l=linux-scsi&m=112540053711489&w=2
MANDRIVA:MDKSA-2006:123

URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:123
REDHAT:RHSA-2006:0493
URL:http://www.redhat.com/support/errata/RHSA-2006-0493.html
SUSE: http://www.novell.com/linux/security/advisories/2006_42_kernel.html
URL:http://www.novell.com/linux/security/advisories/2006_42_kernel.html
SUSE:SUSE-SA:2006:042
URL:http://www.novell.com/linux/security/advisories/2006_42_kernel.html
SUSE:SUSE-SA:2006:047
URL:http://www.novell.com/linux/security/advisories/2006_47_kernel.html
UBUNTU:USN-302-1
URL:http://www.ubuntu.com/usn/usn-302-1
BID:18101
URL:http://www.securityfocus.com/bid/18101
FRSIRT:ADV-2006-3330
URL:http://www.frsirt.com/english/advisories/2006/3330
SECUNIA:20237
URL:http://secunia.com/advisories/20237
SECUNIA:20716
URL:http://secunia.com/advisories/20716
SECUNIA:21045
URL:http://secunia.com/advisories/21045
SECUNIA:21179
URL:http://secunia.com/advisories/21179
SECUNIA:21555
URL:http://secunia.com/advisories/21555
XF:kernel-sg-dos(28510)
URL:http://xforce.iss.net/xforce/xfdb/28510

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-1528

❖ 16317 Linux Kernel Uncleared HID0[31] Denial of Service Vulnerability

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

The vulnerability is caused due to an error on PPC970 when the support processor attention enable bit (HID0[31]) is set.

Successful exploitation causes the system to stop responding.

The vulnerability has been reported in versions prior to 2.6.17.9 or 2.4.33.1.

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

References:

Original advisory:
http://kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.33.1
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.17.9

Other references:
BID:19615
URL:http://www.securityfocus.com/bid/19615
FRSIRT:ADV-2006-3330
URL:http://www.frsirt.com/english/advisories/2006/3330
FRSIRT:ADV-2006-3331
URL:http://www.frsirt.com/english/advisories/2006/3331
SECUNIA:21563
URL:http://secunia.com/advisories/21563

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-4093

❖ 16318 Linux Kernel Ext3 Invalid Inode Number Denial of Service

James McKenzie has reported a vulnerability in Linux Kernel, which can be exploited by malicious users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in ext3 when handling an invalid inode number. This can be exploited by sending a specially crafted NFS request with a V2 procedure (e.g. V2_LOOKUP) that specifies an invalid inode number.

Successful exploitation causes the exported directory to be remounted read-only.

The vulnerability has been reported in versions 2.6.14.4, 2.6.17.6, and 2.6.17.7. Other versions may also be affected.

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

References:

Original advisory:
http://lkml.org/lkml/2006/7/17/41

Other references:
MISC: https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=199172
MANDRIVA:MDKSA-2006:150
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:150
MANDRIVA:MDKSA-2006:151
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:151
REDHAT:RHSA-2006:0617
URL:http://www.redhat.com/support/errata/RHSA-2006-0617.html
TRUSTIX:2006-0046
URL:http://www.trustix.org/errata/2006/0046/
SECUNIA:21369
URL:http://secunia.com/advisories/21369
SECUNIA:21605
URL:http://secunia.com/advisories/21605
SECUNIA:21614
URL:http://secunia.com/advisories/21614

Product Homepage:

http://kernel.org/

CVE Reference: CVE-2006-3468

New Vulnerabilities found this Week

Sony PSP TIFF Image Viewing Code Execution Vulnerability

"Execute arbitrary code"

A vulnerability has been discovered in Sony PlayStation Portable, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in libTIFF and can be exploited to execute arbitrary code when a specially crafted TIFF image is viewed in the Photo Viewer.

The vulnerability has been confirmed in version 2.60 and has also been reported in versions 2.00 through 2.80.

References:
http://noobz.eu/content/home.html#280806

IBM AIX dtterm Privilege Escalation Vulnerability

"Gain escalated privileges"

A vulnerability has been reported in IBM AIX, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unspecified error in dtterm and allows execution of arbitrary code with root privileges.

References:
http://www-1.ibm.com/support/docview.wss?uid=isg1IY89052
http://www-1.ibm.com/support/docview.wss?uid=isg1IY89045

X.Org X11 setuid Security Issues

"Escalated privileges"

Some security issues have been reported in X.Org X11, which can be exploited by malicious, local users to perform certain actions with escalated privileges.

The security issues are caused due to missing checks whether the setuid() or similar calls have succeeded. This can be exploited to perform certain actions with root privileges if the calls fail due to e.g. resource limits.

The security issue has been reported in versions 6.7.0 through 7.1.0. Other versions may also be affected.

References:
http://lists.freedesktop.org/archives/xorg/2006-June/016146.html

Cisco VPN 3000 Concentrator FTP Management Vulnerabilities

"Delete configuration files and certificates on the device"

Two vulnerabilities have been reported in Cisco VPN 3000 Concentrator, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerabilities are caused due to unspecified errors when using FTP as a management protocol and can be exploited to run the "CWD", "MKD", "CDUP", "RNFR", "SIZE", and "RMD" commands without being authenticated. This can e.g. be exploited to delete configuration files and certificates on the device.

Successful exploitation requires that the device has been configured to use FTP as a management protocol (default setting).

The vulnerabilities affect models 3005, 3015, 3020, 3030, 3060, and 3080 running the following versions:
* Any version prior to 4.1
* Any 4.1.x version prior to, and including, 4.1(7)L
* Any 4.7.x version prior to, and including, 4.7(2)F

References:
http://www.cisco.com/warp/public/707/cisco-sa-20060823-vpn3k.shtml

Cisco Firewall Products Unintentional Password Modification

"Unauthorized access"

A security issue has been reported in various Cisco Firewall products, which may allow malicious people to bypass certain security restrictions.

The problem is caused due to an error resulting in certain passwords (EXEC password, passwords of locally defined usernames, and the enable password in the start-up configuration) being unintentionally changed to a non-random value without user intervention.

The error may happen during a software crash or multiple users configuring a device at the same time.

This may result in users being locked out or lead to unauthorized access to an affected device.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20060823-firewall.shtml

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