netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 40

October 12, 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

UK customers want safe data. Too many cooks...Small gang behind recent phishing surge. Experts question whether PCI certification actually improves security.

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

❖ Data security is key to UK consumers' trust

Safeguarding customer data should be a priority for UK companies — because consumers here place great store on how businesses treat their information, according to research.

Out of eight European nations, UK nationals stand out as the most concerned their data is kept safe.

Eighty-one per cent of Britons polled by Unisys said an organisation's ability to keep their data safe is a key trust-building attribute. This compares to 42 percent of French respondents, 40 percent of Belgians and 35 percent of German consumers.

ZDNet

Full Story :
http://news.zdnet.co.uk/security/0,1000000189,39289935,00.htm

❖ Too many cooks will spoil ID fraud broth

Calls for an ID tsar to tackle the growing problem of identity fraud are misjudged.
The idea is being proposed by an all-party committee of MPs to provide a fulcrum for a problem that touches such a wide range of issues. So far, so good.

But in reality, the high-tech crime arena already suffers from too many, rather than too few, focal points.

It is an impressive list: the Serious Fraud Office, the Information Commissioner, the former National Hi-Tech Crime Unit (NHCTU) now absorbed into the Serious Organised Crime Agency, the fledgling National eCrime Co-ordination Unit being set up at the Metropolitan Police to replace the management aspect of NHCTU's role.
With so many co-ordinators already, is there really room, let alone a requirement, for more?

vnunet

Full Story :
http://www.vnunet.com/computing/analysis/2200943/cooks-spoil-id-fraud-broth

❖ Security experts: Rock Phish is behind growing 'Net fraud

SAN FRANCISCO — A recent surge in phishing — fraudulent e-mail and websites designed to "fish" sensitive personal information such as passwords and credit card numbers — is the handiwork of a small, shadowy cybergang, computer security experts say.

Rock Phish, a group of technically savvy hackers who oversee phishing websites and provide tools on the Internet that let others phish, is "the major driving force behind a worsening situation, and they are difficult to track down," says Zulfikar Ramzan, senior principal researcher at Symantec's (SYMC) Security Response Group.

Usa today

Full Story :
http://www.usatoday.com/tech/news/computersecurity/2007-10-10-rock-fish_N.htm

❖ Security Experts: Merchants Racing to the Bottom for PCI Certs

Some security experts say merchants put getting PCI-certified above actually improving security.

Security experts are starting to grumble about the Payment Card Industry Data Security Standard, saying that some merchants just want to get PCI-certified as cheaply and easily as possible—and that the PCI certification system is set up to help them do just that.

"The entire system seems to be set up not to find vulnerabilities," Jeremiah Grossman, chief technology officer and founder of WhiteHat Security, based in Santa Clara, Calif., and one of 135 security firms on the PCI Security Council's list of ASVs (Approved Scanning Vendors), said in an interview with eWEEK.

eweek

Full Story :
http://www.eweek.com/article2/0,1895,2194195,00.asp

New Vulnerabilities Tested in SecureScout

❖ 16664 Linux Kernel ptrace Single Step "CS" Null Pointer Dereference

Evan Teran has reported a security issue 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 an error in ptrace when single-stepping a debugged child process with invalid values in the "CS" register, which can be exploited to cause a kernel oops.

The vulnerability is reported in versions prior to 2.6.22.0.

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

References:

* MISC:
http://bugzilla.kernel.org/show_bug.cgi?id=8765
* CONFIRM:
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=29eb51101c02df517ca64ec472d7501127ad1da8
* CONFIRM:
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=a10d9a71bafd3a283da240d2868e71346d2aef6f
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=248324
* DEBIAN: DSA-1378
http://www.debian.org/security/2007/dsa-1378
* UBUNTU: USN-518-1
http://www.ubuntu.com/usn/usn-518-1
* BID: 25801
http://www.securityfocus.com/bid/25801
* SECUNIA: 26935
http://secunia.com/advisories/26935
* SECUNIA: 26955

http://secunia.com/advisories/26955
* SECUNIA: 26978
http://secunia.com/advisories/26978

CVE Reference: CVE-2007-3731

❖ 16663 Linux Kernel ATM module kernel panic Vulnerability

The ATM module in the Linux kernel before 2.4.35.3, when CLIP support is enabled, allows local users to cause a denial of service (kernel panic) by reading /proc/net/atm/arp before the CLIP module has been loaded.

The vulnerability is reported in versions prior to 2.4.35.3 and 2.6.22.7.

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

References:

* MISC:
http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.4.35.y.git;a=commitdiff;h=b7ae15e7707050baafe5a35e3d4f2d175197d222
* CONFIRM:
http://kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.35.3
* CONFIRM:
http://lwn.net/Articles/251162/
* BID: 25798
http://www.securityfocus.com/bid/25798
* FRSIRT: ADV-2007-3246
http://www.frsirt.com/english/advisories/2007/3246

CVE Reference: CVE-2007-5087

❖ 16662 Linux Kernel ptrace Local Privilege Escalation Vulnerability

Wojciech Purczynski 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 the kernel not zero-extending x86_64 registers after ptrace in the 32bit entry path in arch/x86_64/ia32/ia32entry.S on x86_64 platforms.

The vulnerability is reported in versions prior to 2.4.35.3 and 2.6.22.7.

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

References:

* BUGTRAQ: 20070924 COSEINC Linux Advisory #2: IA32 System Call Emulation

Vulnerability
http://www.securityfocus.com/archive/1/archive/1/480451/100/0/threaded
* BUGTRAQ: 20070926 Re: COSEINC Linux Advisory #2: IA32 System CallEmulation Vulnerability
http://www.securityfocus.com/archive/1/archive/1/480705/100/0/threaded
* FULLDISC: 20070924 COSEINC Linux Advisory #2: IA32 System Call
http://marc.info/?l=full-disclosure&m=119062587407908&w=2
* MLIST: [linux-kernel] 20070921 Linux 2.6.22.7
http://lkml.org/lkml/2007/9/21/512

CVE Reference: CVE-2007-4573

❖ 16660 RPC Authentication Vulnerability Could Allow Denial of Service (MS07-058/933729) (Remote File Checking)

A denial of service vulnerability exists in the remote procedure call (RPC) facility due to a failure in communicating with the NTLM security provider when performing authentication of RPC requests. An anonymous attacker could exploit the vulnerability by sending a specially crafted RPC authentication request to a computer over the network. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart.

The issue is fixed in VMware Server 1.0.4 Build 56528.

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

References:

* MS: MS07-058
http://www.microsoft.com/technet/security/Bulletin/MS07-058.mspx

CVE Reference: CVE-2007-2228

❖ 16659 Word Memory Corruption Vulnerability (MS07-060/942695) (Remote File Checking)

A remote code execution vulnerability exists in the way that Word handles specially crafted Word files. The vulnerability could allow remote code execution if a user opens a specially crafted Word file with a malformed string. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS07-060
http://www.microsoft.com/technet/security/bulletin/ms07-060.mspx
* SECUNIA: 27151

http://secunia.com/advisories/27151

CVE Reference: CVE-2007-3899

❖ 16658 Internet Explorer Address Bar Spoofing Vulnerability (CVE-2007-1091/CVE-2007-3826) (MS07-057/939653) (Remote File Checking)

Spoofing vulnerabilities exist in Internet Explorer that could allow an attacker to display spoofed content in a browser window. The address bar and other parts of the trust UI has been navigated away from the attacker's Web site but the content of the window still contains the attacker's Web page.

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

References:

* BUGTRAQ: 20070223 MSIE7 browser entrapment vulnerability (probably Firefox, too)
http://www.securityfocus.com/archive/1/archive/1/461023/100/0/threaded
* BUGTRAQ: 20070223 Secunia Research: Internet Explorer 7 "onunload" Event SpoofingVulnerability
http://www.securityfocus.com/archive/1/archive/1/461027/100/0/threaded
* MISC:
http://lcamtuf.coredump.cx/ietrap
* MS: MS07-057
http://www.microsoft.com/technet/security/bulletin/ms07-057.mspx
* BID: 22680
http://www.securityfocus.com/bid/22680
* FRSIRT: ADV-2007-0713
http://www.frsirt.com/english/advisories/2007/0713
* SECUNIA: 23014
http://secunia.com/advisories/23014
* SREASON: 2291
http://securityreason.com/securityalert/2291
* XF: ie-mozilla-onunload-dos(32647)
http://xforce.iss.net/xforce/xfdb/32647
* XF: ie-mozilla-onunload-url-spoofing(32649)
http://xforce.iss.net/xforce/xfdb/32649
* BUGTRAQ: 20070713 MSIE7 entrapment again (FF tidbit)
http://www.securityfocus.com/archive/1/archive/1/473702/100/0/threaded
* MISC:
http://lcamtuf.coredump.cx/ietrap3/
* BID: 24911
http://www.securityfocus.com/bid/24911
* FRSIRT: ADV-2007-2540
http://www.frsirt.com/english/advisories/2007/2540
* SECUNIA: 26069
http://secunia.com/advisories/26069
* SREASON: 2892
http://securityreason.com/securityalert/2892
* XF: ie-open-addressbar-spoofing(35421)
http://xforce.iss.net/xforce/xfdb/35421

CVE Reference: CVE-2007-1091

❖ 16657 Internet Explorer Error Handling Memory Corruption Vulnerability (MS07-057/939653) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer due to an unhandled error in certain situations. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If a user viewed the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

* MS: MS07-057
http://www.microsoft.com/technet/security/bulletin/ms07-057.mspx

CVE Reference: CVE-2007-3893

❖ 16656 Internet Explorer Address Bar Spoofing Vulnerability (CVE-2007-3892) (MS07-057/939653) (Remote File Checking)

A spoofing vulnerability exists in Internet Explorer that could allow an attacker to display spoofed content in a browser window. The address bar and other parts of the trust UI has been navigated away from the attacker's Web site but the content of the window still contains the attacker's Web page.

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

References:

* MS: MS07-057
http://www.microsoft.com/technet/security/bulletin/ms07-057.mspx

CVE Reference: CVE-2007-3892

❖ 16655 Network News Transfer Protocol Memory Corruption Vulnerability (MS07-056/941202) (Remote File Checking)

A remote code execution vulnerability exists in Outlook Express and Windows Mail for Microsoft Vista, due to an incorrectly handled malformed NNTP response. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If a user viewed the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.

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

References:

* IDEFENSE: 20071009 Microsoft Windows Mail and Outlook Express NNTP Protocol Heap Overflow
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=607
* MS: MS07-056
http://www.microsoft.com/technet/security/bulletin/ms07-056.mspx
* SECUNIA: 27112
http://secunia.com/advisories/27112

CVE Reference: CVE-2007-3897

❖ 16654 Kodak Image Viewer Remote Code Execution Vulnerability (MS07-055/923810) (Remote File Checking)

A remote code execution vulnerability exists in the way that the Kodak Image Viewer in Windows handles specially crafted image files. An attacker could exploit the vulnerability by constructing a specially crafted image that could potentially allow remote code execution if a user visited a Web site, viewed a specially crafted e-mail message, or opened an e-mail attachment. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

* MS: MS07-055
http://www.microsoft.com/technet/security/bulletin/ms07-055.mspx
* SECTRACK: 1018784
http://securitytracker.com/alerts/2007/Oct/1018784.html

CVE Reference: CVE-2007-2217

New Vulnerabilities found this Week

OpenBSD dhcpd Buffer Overflow Vulnerability

"Denial of Service"

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

The vulnerability is caused due to the improper handling of DHCP requests within dhcpd in the "cons_options()" function in options.c. This can be exploited to cause a stack-based buffer overflow by sending a specially crafted DHCP request specifying a maximum message size between DHCP_FIXED_LEN and DHCP_FIXED_LEN + 3.

Successful exploitation may allow the execution of arbitrary code.

References:

http://www.coresecurity.com/index.php5?module=ContentMod&action=item&id=1962

Cisco IOS Line Printer Daemon Buffer Overflow Vulnerability

"Denial of Service"

Andy Davis has reported a vulnerability in Cisco IOS, which potentially can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the LPD service of Cisco IOS when printing an error message containing an overly long (more than 99 bytes) hostname. This can be exploited to cause a stack-based buffer overflow by e.g. connecting to the default LPD port (515/TCP).

Successful exploitation may allow the execution of arbitrary code but requires that the LPD daemon is enabled (disabled by default) and that the attacker can control the hostname of the router.

References:
http://www.irmplc.com/index.php/155-Advisory-024
http://www.cisco.com/warp/public/707/cisco-sr-20071010-lpd.shtml

Microsoft Patch Tuesday

This Tuesday, Microsoft released the following patches and advisories:

* Kodak Image Viewer Remote Code Execution Vulnerability (MS07-055/923810) (Remote File Checking)
* Network News Transfer Protocol Memory Corruption Vulnerability (MS07-056/941202) (Remote File Checking)
* Internet Explorer Address Bar Spoofing Vulnerability (CVE-2007-3892) (MS07-057/939653) (Remote File Checking)
* Internet Explorer Error Handling Memory Corruption Vulnerability (MS07-057/939653) (Remote File Checking)
* Internet Explorer Address Bar Spoofing Vulnerability (CVE-2007-1091/CVE-2007-3826) (MS07-057/939653) (Remote File Checking)
* Word Memory Corruption Vulnerability (MS07-060/942695) (Remote File Checking)
* RPC Authentication Vulnerability Could Allow Denial of Service (MS07-058/933729) (Remote File Checking)

References:
http://www.microsoft.com/technet/security/bulletin/ms07-oct.mspx
http://descriptions.securescout.com/tc/16654
http://descriptions.securescout.com/tc/16655
http://descriptions.securescout.com/tc/16656
http://descriptions.securescout.com/tc/16657
http://descriptions.securescout.com/tc/16658
http://descriptions.securescout.com/tc/16659
http://descriptions.securescout.com/tc/16660

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