netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 38

September 28, 2007

Table of Contents

Product Focus

Spida Digispid Worm Scanner – The Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

This Week in Review

honeynets central in collecting thread data. The September 30 deadline for PCI compliance is up while companies still struggle. A backgrounder on sql-injections. Security succeeds when tailoring systems to users instead of the other way around.

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

- **Cool tools for hacker trackers**

A honeynet reporting site and the latest version of a solid hacking package help security pros
If you want to keep up with the latest criminal exploits without having to collect malware yourself, take a look at SRI International's Cyber-Threat Analytics BotHunter Malware Analysis Web page. Reporting on information and statistics collected from a research honeynet, the BotHunter Malware Analysis page makes daily infection logs

from high-interaction honeypots available for anyone to view. Although the scale of the project and information collected is fairly small, this is a useful site for gaining more insight into crimeware and the world of bots.

infoworld

Full Story :
http://www.infoworld.com/article/07/09/28/39OPsecadvise-bothunter-cainandable_1.html?source=rss&url=http://www.infoworld.com/article/07/09/28/39OPsecadvise-bothunter-cainandable_1.html

❖ Study Shows Businesses Face PCI Challenges

The Sept. 30 deadline set by Visa USA for large enterprises to comply with the Payment Card Industry Data Security Standard is looming. But even with the deadline so close, a study commissioned by EMC's security division found that many businesses are still struggling to make the grade.
The study for RSA Security—performed by Forrester Consulting, which surveyed 677 organizations across the Unite States and Europe—found businesses are facing a number of challenges in achieving compliance.

eweek

Full Story :
http://www.eweek.com/article2/0,1895,2189271,00.asp

❖ Is SQL Injection Still a Major Security Threat?

Robert Graham, CEO of Errata Security, explains SQL injection, a technique criminal hackers could use to compromise Web site databases.
Q: What exactly is SQL injection?
A: SQL injection is a type of attack that targets Web sites backed by a relational database such as Microsoft SQL Server, Oracle or MySQL. The database might be doing nothing more complicated than capturing user names and passwords, or it might be executing full-blown sales transactions.
Q: Who is vulnerable to SQL injection?
A: Hundreds of thousands of sites around the world are potentially vulnerable to SQL injection if they don't properly defend against it.)

eweek

Full Story :
http://www.eweek.com/article2/0,1895,2188714,00.asp

❖ Security experts pitch 'culture of data'

The key to keeping a happy network: Live in your users' reality
The companies that are having the most success in advancing their data security efforts today are those that are finding a way to protect sensitive information without getting in the way of business users, industry experts maintain.

In crafting their data-handling policies and selecting from the multitude of security technologies at their fingertips, those businesses that can foster both ready access to information, along with strong defenses for end-users and IT systems, are making progress the fastest, claim leading vendors and service providers.

After years of "throwing technologies" at the data security problem while juggling complex business demands along with external threats and regulatory compliance audits, some businesses are finally discovering that they can simplify the entire process by taking a more comprehensive approach to tailoring their programs to the manner in which their users access, handle, and share information.

computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9038960&taxonomyId=17&intsrc=kc_feat

New Vulnerabilities Tested in SecureScout

- **16644 VMware Workstation, virtual machine process (VMX) denial of service against the guest Operating System Vulnerability (Remote File Checking)**

VMware Workstation before 5.5.4 allows attackers to cause a denial of service against the guest OS by causing the virtual machine process (VMX) to store malformed configuration information.

The issue is fixed in VMware Workstation 5.5.4.

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

References:

* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html#554
* FRSIRT: ADV-2007-1592
http://www.frsirt.com/english/advisories/2007/1592
* SECTRACK: 1018011
http://www.securitytracker.com/id?1018011
* SECUNIA: 25079
http://secunia.com/advisories/25079
* XF: vmware-vmx-dos(33992)
http://xforce.iss.net/xforce/xfdb/33992

CVE Reference: CVE-2007-1877

- **16643 VMware Workstation, Shared Folders feature Directory traversal Vulnerability (Remote File Checking)**

Directory traversal vulnerability in the Shared Folders feature for VMware Workstation

before 5.5.4, when a folder is shared, allows users on the guest system to write to arbitrary files on the host system via the "Backdoor I/O Port" interface.

The issue is fixed in VMware Workstation 5.5.4.

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

References:

* IDEFENSE: 20070427 VMware Workstation Shared Folders Directory Traversal Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=521
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html#554
* BID: 23721
http://www.securityfocus.com/bid/23721
* FRSIRT: ADV-2007-1592
http://www.frsirt.com/english/advisories/2007/1592
* SECTRACK: 1017980
http://www.securitytracker.com/id?1017980
* SECUNIA: 25079
http://secunia.com/advisories/25079

CVE Reference: CVE-2007-1744

❖ **16642 VMware Workstation, virtual machine process (VMX) Denial of Service Vulnerability (Remote File Checking)**

The virtual machine process (VMX) in VMware Workstation before 5.5.4 does not properly read state information when moving from the ACPI sleep state to the run state, which allows attackers to cause a denial of service (virtual machine reboot) via unknown vectors.

The issue is fixed in VMware Workstation 5.5.4.

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

References:

* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html#554
* FRSIRT: ADV-2007-1592
http://www.frsirt.com/english/advisories/2007/1592
* SECTRACK: 1018011
http://www.securitytracker.com/id?1018011
* SECUNIA: 25079
http://secunia.com/advisories/25079
* XF: vmware-acpi-unspecified(33990)
http://xforce.iss.net/xforce/xfdb/33990

CVE Reference: CVE-2007-1337

❖ 16641 VMware Workstation, guest operating system memory management related Denial of Service Vulnerability (Remote File Checking)

The memory management in VMware Workstation before 5.5.4 allows attackers to cause a denial of service (Windows virtual machine crash) by triggering certain general protection faults (GPF).

The issue is fixed in VMware Workstation 5.5.4.

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

References:

* BUGTRAQ: 20070507 [Reversemode Advisory] VMware Products - GPF Denial of Service
http://www.securityfocus.com/archive/1/archive/1/467836/100/0/threaded
* MISC:
http://www.reversemode.com/index.php?option=com_remository&Itemid=2&func=fileinfo&id=49
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html#554
* FRSIRT: ADV-2007-1592
http://www.frsirt.com/english/advisories/2007/1592
* SECTRACK: 1018011
http://www.securitytracker.com/id?1018011
* SECUNIA: 25079
http://secunia.com/advisories/25079
* XF: vmware-gpf-dos(33994)
http://xforce.iss.net/xforce/xfdb/33994

CVE Reference: CVE-2007-1069

❖ 16639 VMware Workstation, Unquoted Windows search path, privileges escalation Vulnerability (Remote File Checking)

Unquoted Windows search path vulnerability in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017 allows local users to gain privileges unspecified vectors, possibly involving a malicious "program.exe" file in the C: folder.

The issue is fixed in VMware Workstation 5.5.5 Build 56455 and 6.0.1 Build 55017.

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

References:

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html
* CONFIRM:
http://www.vmware.com/support/player/doc/releasenotes_player.html
* CONFIRM:
http://www.vmware.com/support/player2/doc/releasenotes_player2.html
* CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html
* CONFIRM:
http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html
* BID: 25732
http://www.securityfocus.com/bid/25732

CVE Reference: CVE-2007-5023

❖ 16638 VMware Workstation, Denial of Service on guest operating system Vulnerability (Remote File Checking)

Unspecified vulnerability in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017 allows users with login access to a guest operating system to cause a denial of service (guest outage and host process crash or hang) via unspecified vectors.

The issue is fixed in VMware Workstation 5.5.5 Build 56455 and 6.0.1 Build 55017.

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

References:

* CONFIRM:
http://www.vmware.com/support/ace/doc/releasenotes_ace.html
* CONFIRM:
http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html
* CONFIRM:
http://www.vmware.com/support/player/doc/releasenotes_player.html
* CONFIRM:
http://www.vmware.com/support/player2/doc/releasenotes_player2.html
* CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html
* CONFIRM:
http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html
* BID: 25731
http://www.securityfocus.com/bid/25731

CVE Reference: CVE-2007-4497

❖ 16637 VMware Workstation, Memory corruption and arbitrary code execution on the host operating system Vulnerability (Remote File Checking)

Unspecified vulnerability in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017 allows authenticated users with administrative privileges on a guest operating system to corrupt memory and possibly execute arbitrary code on the host operating system via unspecified vectors.

The issue is fixed in VMware Workstation 5.5.5 Build 56455 and 6.0.1 Build 55017.

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

References:

* CONFIRM:
http://www.vmware.com/support/ace/doc/releasenotes_ace.html
* CONFIRM:
http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html
* CONFIRM:
http://www.vmware.com/support/player/doc/releasenotes_player.html
* CONFIRM:
http://www.vmware.com/support/player2/doc/releasenotes_player2.html
* CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html
* CONFIRM:
http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html
* BID: 25728
http://www.securityfocus.com/bid/25728

CVE Reference: CVE-2007-4496

❖ 16636 VMware Workstation, DHCP server Integer underflow, arbitrary code execution Vulnerability (Remote File Checking)

Integer overflow in the DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017 allows remote attackers to execute arbitrary code via a malformed DHCP packet that triggers a stack-based buffer overflow.

The issue is fixed in VMware Workstation 5.5.5 Build 56455 and 6.0.1 Build 55017.

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

References:

* ISS: 20070919 VMWare DHCP Server Remote Code Execution Vulnerabilities
http://www.iss.net/threats/275.html
* CONFIRM:
http://www.vmware.com/support/ace/doc/releasenotes_ace.html
* CONFIRM:
http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html
* CONFIRM:
http://www.vmware.com/support/player/doc/releasenotes_player.html
* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html
* CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html
* CONFIRM:
http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html
* BID: 25729
http://www.securityfocus.com/bid/25729
* XF: dhcp-param-underflow(33103)
http://xforce.iss.net/xforce/xfdb/33103

CVE Reference: CVE-2007-0063

❖ 16635 VMware Workstation, DHCP server Integer overflow, arbitrary code execution Vulnerability (Remote File Checking)

Integer overflow in the DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017 allows remote attackers to execute arbitrary code via a malformed DHCP packet that triggers a stack-based buffer overflow.

The issue is fixed in VMware Workstation 5.5.5 Build 56455 and 6.0.1 Build 55017.

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

References:

* ISS: 20070919 VMWare DHCP Server Remote Code Execution Vulnerabilities
http://www.iss.net/threats/275.html
* CONFIRM:
http://www.vmware.com/support/ace/doc/releasenotes_ace.html
* CONFIRM:
http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html
* CONFIRM:
http://www.vmware.com/support/player/doc/releasenotes_player.html
* CONFIRM:
http://www.vmware.com/support/player2/doc/releasenotes_player2.html
* CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html
* CONFIRM:
http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html
* BID: 25729
http://www.securityfocus.com/bid/25729
* XF: dhcp-param-overflow(33102)
http://xforce.iss.net/xforce/xfdb/33102

CVE Reference: CVE-2007-0062

❖ 16634 VMware Workstation, DHCP server arbitrary code execution Vulnerability (Remote File Checking)

The DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 55017 allows remote attackers to execute arbitrary code via a malformed packet that triggers "corrupt stack memory."

The issue is fixed in VMware Workstation 5.5.5 Build 56455 and 6.0.1 Build 55017.

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

References:

* ISS: 20070919 VMWare DHCP Server Remote Code Execution Vulnerabilities
http://www.iss.net/threats/275.html
* CONFIRM:
http://www.vmware.com/support/ace/doc/releasenotes_ace.html
* CONFIRM:
http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html
* CONFIRM:
http://www.vmware.com/support/player/doc/releasenotes_player.html
* CONFIRM:
http://www.vmware.com/support/player2/doc/releasenotes_player2.html
* CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html
* CONFIRM:
http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html
* BID: 25729
http://www.securityfocus.com/bid/25729
* XF: dhcp-malformed-packet-bo(33101)
http://xforce.iss.net/xforce/xfdb/33101

CVE Reference: CVE-2007-0061

New Vulnerabilities found this Week

Cisco Catalyst 6500 / Cisco 7600 Series Devices Accessible Loopback Address Weakness

"Bypass existing access control lists"

A weakness has been reported in Cisco Catalyst 6500 and Cisco 7600 series devices, which can be exploited by malicious people to bypass certain security restrictions.

The problem is that packets destined for the 127.0.0.0/8 network may be received and processed by e.g. the Supervisor module or Multilayer Switch Feature Card (MSFC). This can be exploited to e.g. bypass existing access control lists.

Successful exploitation requires that systems are running Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the MSFC) or Native

Mode (IOS Software on both the Supervisor Engine and the MSFC).

The weakness is reported in all software versions on Cisco Catalyst 6500 and Cisco 7600 series prior to 12.2(33)SXH.

References:
http://www.cisco.com/warp/public/707/cisco-sr-20070926-lb.shtml

F-Secure Archives and Packed Executables Detection Bypass

"Bypass the anti-virus scanning functionality"

A vulnerability has been reported in F-Secure Anti-Virus, which can be exploited by malware to bypass the scanning functionality.

The vulnerability is caused due to an unspecified error in the handling of archives and packed executables. This can be exploited to bypass the anti-virus scanning functionality by placing specially crafted archives or packed executables in the "system32" directory.

The vulnerability only affects 64-bit server platforms.

The vulnerability is reported in F-Secure Anti-Virus for Windows Servers version 7.00.

References:
http://www.f-secure.com/security/fsc-2007-6.shtml

PHP-Nuke Dance Music Module Local File Inclusion

"Disclose sensitive information"

Janek Vind has discovered a vulnerability in the Dance Music module for PHP-Nuke, which can be exploited by malicious people to disclose sensitive information.

Input passed to the "ACCEPT_FILE[1]" parameter through modules.php in the PHP-Nuke installation to index.php in the module (when "page" is set to "1") is not properly verified before being used to include files. This can be exploited to include arbitrary files from local resources.

The vulnerability is confirmed in version 1.0. Other versions may also be affected.

References:
http://www.waraxe.us/advisory-54.html

Sun StarOffice Office Suite TIFF Parsing Integer Overflow Vulnerabilities

"Execution of arbitrary code"

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

The vulnerabilities are caused due to integer overflows when processing certain tags within TIFF images. This can be exploited to cause heap-based buffer overflows by e.g. tricking a user into opening a specially crafted document.

Successful exploitation may allow the execution of arbitrary code.

The vulnerabilities are reported in StarOffice 6.0 Office Suite, StarOffice 7 Office Suite, and StarOffice 8 Office Suite.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102994-1
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=593

HP TCP/IP Services for OpenVMS BIND Vulnerability

"Poison the DNS cache"

HP has acknowledged a vulnerability in HP OpenVMS, which can be exploited by malicious people to poison the DNS cache.

References:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01174368

PHP-Nuke Nuke Mobile Entertainment Module Local File Inclusion

"Include arbitrary files"

BorN To K!LL has discovered a vulnerability in the Nuke Mobile Entertainment module for PHP-Nuke, which can be exploited by malicious people to disclose sensitive information.

Input passed to the "module_name" parameter in data/compatible.php is not properly verified before being used to include files. This can be exploited to include arbitrary files from local resources.

Successful exploitation requires that "register_globals" is enabled and "magic_quotes_gpc" is disabled, which are not the values recommended by the PHP-Nuke installer.

References:
http://milw0rm.com/exploits/4447

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.

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