netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 39

October 05, 2007

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

Web developers ignore security flaws. Here are some strong opinions on how to obtain security. Who should store our credit card information? Can new hardware stop viruses?

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 top 10 reasons Web sites get hacked**

Web developers ignore security flaws at customers' peril
Web security is at the top of customers' minds after many well-publicized personal data breaches, but the people who actually build Web applications aren't paying much attention to security, experts say.

"They're totally ignoring it," says IT consultant Joel Snyder. "When you go to your Web site design team, what you're looking for is people who are creative and able to

build these interesting Web sites... That's No. 1, and No. 9 on the list would be that it's a secure Web site." Read the latest WhitePaper - State of Internet Security Report on Protecting Enterprise Systems

PC World

Full Story :
http://www.pcworld.idg.com.au/index.php/id;1126870565

❖ One of the main problems is...

99% (whatever, a huge number) of the people out there running regular desktop or laptop computers need a secure *internet appliance that doesn't suck*. We have good enough tech now to make appliances that are fast and functional and reboot into a fresh clean install as often as they are turned on and off. Live CDs and enough ram, you don't need a permanent hard drive install.

Previous appliances have sucked, web Tv-no mouse?? Whut the heck? and so on, anemic processors, dismal RAM amount, frankly just plain wrong OS, no apps.

Times change. You can have a full featured computer like experience that is basically immune to any permanent infestation, with no hoop jumping required, they could make it dogsquat simple, literally an on off button like any other appliance.

technocrat

Full Story :
http://technocrat.net/d/2007/10/4/28196

❖ Retailers, credit card industry clash on data security standards

BOSTON - Retailers and the credit card industry are at odds as they try to restore consumer confidence after recent massive thefts of credit card information.

The National Retail Federation on Thursday urged a card industry organization to stop requiring retailers to keep customers' card numbers for up to 18 months.

The stored data helps track product returns and disputed or suspicious transactions. But retailers say the data would be more secure if only credit card companies and banks that issue the cards stored it.

"It makes more sense for credit card companies to protect their data from thieves by keeping it in a relatively few secure locations than to expect millions of merchants scattered across the nation to lock up their data for them," David Hogan, the retail federation's chief information officer, said in a strongly worded letter.

Mercury News

Full Story :
http://www.mercurynews.com/ci_7091053?source=rss

- **Multicore CPUs hold key to stopping viruses**

NEC's technique isolates single cores once they are infected
As any tech-head will know, there are plenty of recent PCs that run speedy and efficient multicore CPUs, but who would have thought that such chips will soon be appearing in mobile phones, cars and HD TV players and that they could hold the key to eliminating computer viruses?

According to NEC Japan, its new technique [Subscription link] for running software in separate processes on each core of a multicore CPU opens the door to stopping a virus before it spreads throughout any internet-connected device.

Tech.co.uk

Full Story :
http://www.tech.co.uk/computing/upgrades-and-peripherals/processors/news/multicore-cpus-hold-key-to-stopping-viruses?articleid=802567027&source=rss

New Vulnerabilities Tested in SecureScout

- **16653 VMware GSX Server, Heap-based buffer overflow in the NAT networking components Vulnerability (Remote File Checking)**

Heap-based buffer overflow in the NAT networking components vmnat.exe and vmnet-natd in VMWare GSX Server 3.2 allows remote authenticated attackers, including guests, to execute arbitrary code via crafted EPRT and PORT FTP commands.

The issue is fixed in VMware GSX Server 3.2.1.

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

References:

* BUGTRAQ: 20051221 VMware vulnerability in NAT networking
http://www.securityfocus.com/archive/1/archive/1/420017/100/0/threaded
* FULLDISC: 20051221 [ACSSEC-2005-11-25-0x1] VMWare Workstation 5.5.0 <= build-18007 G SX Server Variants And Others
http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040442.html
* BUGTRAQ: 20051221 [Security-Advisories (at) acs-inc (dot) com [email concealed]: [Full-disclosure] [ACSSEC-2005-11-25-0x1] VMWare Workstation 5.5.0 <= build-18007 G SX Server Variants And Others]
http://www.securityfocus.com/archive/1/archive/1/419997/100/0/threaded
* CONFIRM:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=2000
* GENTOO: GLSA-200601-04
http://www.gentoo.org/security/en/glsa/glsa-200601-04.xml
* CERT-VN: VU#856689
http://www.kb.cert.org/vuls/id/856689
* BID: 15998
http://www.securityfocus.com/bid/15998

* FRSIRT: ADV-2005-3013
http://www.frsirt.com/english/advisories/2005/3013
* SECTRACK: 1015401
http://securitytracker.com/id?1015401
* SECUNIA: 18162
http://secunia.com/advisories/18162
* SECUNIA: 18344
http://secunia.com/advisories/18344
* SREASON: 282
http://securityreason.com/securityalert/282
* SREASON: 289
http://securityreason.com/securityalert/289

CVE Reference: CVE-2005-4459

❖ 16652 VMware Workstation, Heap-based buffer overflow in the NAT networking components Vulnerability (Remote File Checking)

Heap-based buffer overflow in the NAT networking components vmnat.exe and vmnet-natd in VMWare Workstation 5.5 allows remote authenticated attackers, including guests, to execute arbitrary code via crafted EPRT and PORT FTP commands.

The issue is fixed in VMware Workstation 5.5.1.

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

References:

* BUGTRAQ: 20051221 VMware vulnerability in NAT networking
http://www.securityfocus.com/archive/1/archive/1/420017/100/0/threaded
* FULLDISC: 20051221 [ACSSEC-2005-11-25-0x1] VMWare Workstation 5.5.0 <= build-18007 G SX Server Variants And Others
http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040442.html
* BUGTRAQ: 20051221 [Security-Advisories (at) acs-inc (dot) com [email concealed]: [Full-disclosure] [ACSSEC-2005-11-25-0x1] VMWare Workstation 5.5.0 <= build-18007 G SX Server Variants And Others]
http://www.securityfocus.com/archive/1/archive/1/419997/100/0/threaded
* CONFIRM:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=2000
* GENTOO: GLSA-200601-04
http://www.gentoo.org/security/en/glsa/glsa-200601-04.xml
* CERT-VN: VU#856689
http://www.kb.cert.org/vuls/id/856689
* BID: 15998
http://www.securityfocus.com/bid/15998
* FRSIRT: ADV-2005-3013
http://www.frsirt.com/english/advisories/2005/3013
* SECTRACK: 1015401
http://securitytracker.com/id?1015401
* SECUNIA: 18162
http://secunia.com/advisories/18162

* SECUNIA: 18344
http://secunia.com/advisories/18344
* SREASON: 282
http://securityreason.com/securityalert/282
* SREASON: 289
http://securityreason.com/securityalert/289

CVE Reference: CVE-2005-4459

❖ 16651 VMware Server, passwords written in cleartext Vulnerability (Remote File Checking)

EMC VMware Server before 1.0.4 Build 56528 writes passwords in cleartext to unspecified log files, which allows local users to obtain sensitive information by reading these files.

The issue is fixed in VMware Server 1.0.4 Build 56528.

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

References:

* CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html

CVE Reference: CVE-2007-5024

❖ 16650 VMware Server, Unquoted Windows search path, privileges escalation Vulnerability (Remote File Checking)

Unquoted Windows search path vulnerability in EMC VMware Server before 1.0.4 Build 56528 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 Server 1.0.4 Build 56528.

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

❖ 16649 VMware Server, Denial of Service on guest operating system Vulnerability (Remote File Checking)

Unspecified vulnerability in EMC VMware Server before 1.0.4 Build 56528 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 Server 1.0.4 Build 56528.

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

❖ 16648 VMware Server, Memory corruption and arbitrary code execution on the host operating system Vulnerability (Remote File Checking)

Unspecified vulnerability in EMC VMware Server before 1.0.4 Build 56528 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 Server 1.0.4 Build 56528.

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

❖ 16647 VMware Server, DHCP server Integer underflow, arbitrary code execution Vulnerability (Remote File Checking)

Integer overflow in the DHCP server in EMC VMware Server before 1.0.4 Build 56528 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 Server 1.0.4 Build 56528.

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

❖ 16646 VMware Server, DHCP server Integer overflow, arbitrary code execution Vulnerability (Remote File Checking)

Integer overflow in the DHCP server in EMC VMware Server before 1.0.4 Build 56528 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 Server 1.0.4 Build 56528.

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

❖ 16645 VMware Server, DHCP server arbitrary code execution Vulnerability (Remote File Checking)

The DHCP server in EMC VMware Server before 1.0.4 Build 56528 allows remote attackers to execute arbitrary code via a malformed packet that triggers "corrupt stack memory."

The issue is fixed in VMware Server 1.0.4 Build 56528.

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

❖ 16640 VMware Workstation, vstor-ws60.sys host operating system Denial of Service and escalated privileges Vulnerability (Remote File Checking)

vstor-ws60.sys in VMWare Workstation 6.0 allows local users to cause a denial of service (host operating system crash) and possibly gain escalated privileges by sending a small file buffer size value to the FsSetVolumeInformation IOCTL handler with an FsSetFileInformation subcode.

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

References:

* BUGTRAQ: 20070824 security vulnerability in VMware
http://marc.info/?l=bugtraq&m=118805138626360&w=2
* MISC:
http://tarrysingh.blogspot.com/2007/08/security-vmware-workstation-6.html
* BID: 25441
http://www.securityfocus.com/bid/25441
* FRSIRT: ADV-2007-2992
http://www.frsirt.com/english/advisories/2007/2992
* SECTRACK: 1018609
http://www.securitytracker.com/id?1018609
* SECUNIA: 26606

http://secunia.com/advisories/26606
* XF: vmware-vmstor-privilege-escalation(36277)
http://xforce.iss.net/xforce/xfdb/36277

CVE Reference: CVE-2007-4591

New Vulnerabilities found this Week

Apple iPhone Multiple Vulnerabilities
"Cross-site scripting attacks; Disclose sensitive information; Bypass security restrictions; Denial of Service"

Some vulnerabilities, security issues, and a weakness have been reported in the Apple iPhone, which can be exploited by malicious people to conduct cross-site scripting attacks, disclose sensitive information, bypass certain security restrictions, cause a DoS (Denial of Service), or to compromise a vulnerable system.

1) An input validation error when handling SDP (Service Discovery Protocol) packets exists in the iPhone's Bluetooth server. This can be exploited by an attacker in Bluetooth range to cause the application to crash or to execute arbitrary code by sending specially crafted SDP packets.

Successful exploitation requires that Bluetooth is enabled.

2) The problem is that users are not notified about changes of mail servers' identities when Mail is configured to use SSL for incoming and outgoing connections. This can be exploited e.g. to impersonate the user's mail server and obtain the user's email credentials.

Successful exploitation requires a MitM (Man-in-the-Middle) attack.

3) It is possible to cause the iPhone to call a phone number without user confirmation by enticing a user to follow a "tel:" link in a mail message.

4) An error in Safari in the handling of new browser windows can be exploited to disclose the URL of an unrelated page.

5) An error in Safari in the handling of "tel:" links can be exploited to cause the iPhone to dial a different number than the one being displayed in the confirmation dialog. Exiting Safari during the confirmation process may result in unintentional confirmation.

6) An error in Safari can be exploited to set Javascript window properties of pages served from other websites when a malicious web site is viewed.

7) Disabling Javascript in Safari does not take effect until Safari is restarted.

8) An error in Safari allows a malicious website to bypass the same-origin policy using "frame" tags. This can be exploited to execute Javascript code in the context of another site when a user visits a malicious web page.

9) An error in Safari allows Javascript events to be associated with the wrong frame. This can be exploited to execute Javascript code in context of another site when a user visits a malicious web page.

10) An error in Safari allows content served over HTTP to alter or access content served over HTTPS in the same domain. This can be exploited to execute Javascript code in context of HTTPS web pages in that domain when a user visits a malicious web page.

References:
http://docs.info.apple.com/article.html?artnum=306586

Sun Java JRE Multiple Vulnerabilities

"Bypass security restrictions; Manipulate data; Disclose sensitive information"

Multiple vulnerabilities have been reported in Sun Java JRE (Java Runtime Environment), which can be exploited by malicious people to bypass certain security restrictions, manipulate data, disclose sensitive/system information, or potentially compromise a vulnerable system.

1) Multiple unspecified errors in the Java Runtime Environment can be exploited by e.g. a malicious applet or by using Java APIs to establish network connections to certain services on machines other than the originating host.

2) Multiple unspecified errors in Java Web Start can be exploited by a malicious applet to read/write local files or determine the location of the Java Web Start cache.

3) An unspecified error in the Java Runtime Environment can be exploited to move or copy arbitrary files on the system by e.g. tricking a user into dragging and dropping a file from an applet to a desktop application that has the proper permissions.

The vulnerabilities are reported in the following versions:
* JDK and JRE 6 Update 2 and earlier
* JDK and JRE 5.0 Update 12 and earlier
* SDK and JRE 1.4.2_15 and earlier
* SDK and JRE 1.3.1_20 and earlier

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-103079-1
http://sunsolve.sun.com/search/document.do?assetkey=1-26-103078-1
http://sunsolve.sun.com/search/document.do?assetkey=1-26-103073-1
http://sunsolve.sun.com/search/document.do?assetkey=1-26-103072-1

Google Mini Search Appliance "ie" Cross-Site Scripting Vulnerability

"Cross-site scripting attacks"

A vulnerability has been reported in Google Mini Search Appliance, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed to the "ie" parameter when performing a search is not properly sanitised 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.

Example:

http://[site]/search?ie=[code]&site=x&output=xml_no_dtd'&client=x&proxystylesheet=x'

The vulnerability affects Google Mini Search Appliance version 3.4.14.

References:
https://support.google.com/enterprise/doc/mini/advisories/ga-2007-09-m.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