

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[WinHoneyd v1.5b](#) - Download WinHoneyd executable package by filling our download form. Size: 2404KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winhoneyd-1.5b.zip>

This Week in Review

A new threat to be aware of. How they trade your personal info. Law on encrypted personal data communication needs adjustment. Users are still not security savvy.

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

• "Clickjacking" poses major web browser threat

"Clickjacking" has the potential to affect users of nearly all internet browsers.

Clickjacking occurs when an attacker places an invisible button under an internet user's mouse pointer just above the viewable content of the web page, Jeremiah Grossman, founder and CTO of WhiteHat Security, said in an email to SCMagazineUS.com Monday.

The attacker then waits for the user to mistakenly click the button, which can be placed anywhere on any website, Grossman said.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Clickjacking-poses-major-web-browser-threat/article/118487/>

• How 'carders' trade your stolen personal info

Debit cards and PINs are hot subjects on the criminal underground forums these days, Tom Rusin said on a recent visit to CNET. Rusin is president of North American operations at Affinion Group, a company that monitors the criminal underground for several thousand banking institutions by lurking in carder chat rooms.

While scrolling through posts in an online underground criminal forum on his laptop, Rosin explained that since "every American keeps some money in their savings account," unlike when stealing credit cards, debit cards grant thieves immediate access to cash. Next in demand are usernames and passwords because "most people use the same password on the sites they visit."

Cnet Security

Full Story :

http://news.cnet.com/8301-10789_3-10053523-57.html?part=rss&tag=feed&subj=DefenseinDepth

• Nevada mandates encrypted personal data communication

A Nevada law placing restrictions on the transfer of customer's personal information through electronic transmission went into effect on Wednesday.

Rod Murchison, vice president of marketing and strategic alliances at Code Green Networks, provider of data loss prevention solutions, said the law is ambiguous because some of the terms, including "customer" and "electronic transmission" are not defined. He said "electronic transmission" means email, but it also might include file transferring in instant messaging programs, postings to social networking sites or blogs and more.

Murchison said the law is also vague because it does not specify the penalties for not complying. Since the penalties are unspecified, this possibly, "leaves the door wide open for consumers to sue companies for sending out their data," Murchison said.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Nevada-mandates-encrypted-personal-data-communication/article/118630/>

• Many computer users lack basic security precautions, survey says

October 2, 2008 (IDG News Service) Cybersecurity efforts in the U.S. government and among many businesses are improving, but many individual computer users still don't take basic precautions against cyberattacks, cybersecurity experts said Thursday.

His comments came during an event to mark the beginning of the fifth annual National Cyber Security Month.

The National Cyber Security Alliance, one of the groups promoting National Cyber Security Month, recommends that home computer users, at a minimum, have up-to-date antivirus, antispyware and firewall software installed, said Michael Kaiser, NCSA's executive director. Those three software packages won't provide "bullet-proof" protection, but will guard against most cyberattacks, he said.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9116083&source=rss_topic1

• Opinion: Famous tech myths that just won't die

September 26, 2008 (Computerworld) Have you heard this story? One day, Bill Gates was standing on a street corner, watching the clouds roll by. Absentmindedly, he dropped a \$1,000 bill out of his pocket. A bystander noticed and said, "Are you going to pick that up?" "No, why would I do that?" Gates responded gruffly, and walked away. OK, fact or fiction? While my version adds a little color, it's still just a fable. You can mix and match the details, but the essence of the myth -- which I'll define as anything grossly inaccurate yet widely regarded as true -- is still there. It's part fantasy, part fabrication, but wholly inaccurate. Tech myths come in all shapes and sizes: Some contain a morsel of truth, but many of them are so wildly preposterous that it's hard to imagine anyone taking them seriously. "A myth generally exists to explain the worldview of a group of people," says Rob Enderle, a consumer analyst. "This means its intent is to convey an idea but not necessarily the whole truth, and given it's conveyed largely from person to person, the initial story can change a great deal." At the risk of perpetuating Internet-sized myths even more, here are some of the most famous examples of myths, along with some debunking and comments from those in the know. Bill Gates dropped a \$1,000 bill and didn't bother to pick it up Bill Gates is one of the richest people on the planet, but the myth that he would drop a \$1,000 bill and not pick it up probably originated in an e-mail scam. (Click on image for more information about this myth.) (Photo courtesy of World Economic Forum) There's really no factual evidence for this one. If it happened, there's no way to prove it. Given the fact that the U.S. Treasury stopped producing \$1,000 bills during World War II and stopped distributing them in 1969, it seems very unlikely Gates would carry one around. Yet, this and many other myths about Bill Gates -- many of them related to e-mail scams -- seem to become memes faster than other mean-spirited tech gossip. Apparently, Gates is just an easy target who represents how an average guy (albeit

one who is obviously very intelligent) can attain fame and fortune in the tech industry. Those who perpetuate the rumors are probably a little jealous. For its part, Microsoft told me that, officially, it doesn't comment on Bill Gates' personal life. Another Gates myth is that he said "640k ought to be enough for anybody" when talking about an IBM PC's memory in 1981. The iPhone 3G has a kill switch that Apple can use to disable the device Is there a kill switch? (Click on image for more information about this myth.) As with many myths, this one has a modicum of truth. The reality, however, is much less interesting than the myth. You can imagine Steve Jobs cackling to himself as he calls up an unsuspecting iPhone user on a giant screen and then, after pressing a button, watches as the hapless victim struggles to make a phone call. As reported by The Wall Street Journal, the kill switch is actually just a way to disable certain unapproved apps that are used for hacking. The company can't disable the phone at will, and calling software that disables malicious code a "kill switch" seems like a stretch. (I contacted Apple for an official statement, but it hasn't responded yet.) Internet2 will replace the Internet Internet2 runs through major swathes of the U.S., but the pipelines are owned by a collective headed by colleges and universities and there are no plans to make it public. (Click on image for more information about this myth.) Ask a nontechnie if something called Internet2 will one day replace Internet1 and that person will surely concur that it makes sense. Internet2 is actually a private network for a group of partners headed by colleges and universities and has no plans to ever go public. In fact, the costs associated with Internet2 are so exorbitant (some connections run over 1Gbit/sec.) that it would likely take an act of Congress to make it freely available. And even then, the costs to run a public Internet at Internet2 speeds would be too high for ISPs and consumers. And one further point: If Internet2 were the intended successor to the current Internet, companies like Sprint, Verizon and Clearwire wouldn't be busily laying the foundation for 100Mbit/sec. Internet. They would just wait for Internet2 to arrive. PC gaming is dying or already dead EBgames.com lists hundreds of upcoming PC games. True, when the top listing is a prison tycoon game, it doesn't look good. But when EBgames removes the PC gaming section entirely, it might be time to declare the platform dead for games. (Click on image for more information about this myth.) Every major PC gaming magazine, and a few dead ones, have reported on the demise of PC gaming. It's definitely not a happy time to be a keyboard-and-mouse gamer, especially when a site like VG Chartz, which tracks game sales, doesn't even include the platform. Yet, while PC game sales have declined, there still are millions of Mac and PC gamers around. EBgames.com lists no fewer than 170 pages of upcoming PC game titles, and franchises such as The Sims (a new Sims 3 version comes out this fall) and Civilization enjoy a loyal following. Casual PC gaming is also exploding, and sites such as Club Penguin and Barbie.com are overloaded with young PC gamers every day. Apple is working on a MacTablet Apple has already released a MacTablet -- it's called the iPod Touch, which is more portable than a tablet PC, plays music and movies, and uses your fingers as an input device. (Click on image for more information about this myth.) Ah, yes. The elusive MacTablet. In many ways, the iPod Touch and the iPhone itself are better tablet computers than tablet PCs. They are small enough to carry around all day, can be used to browse the Internet and play music, and respond to finger input. Microsoft has never gained any traction with its Tablet PC. If you buy one today, it comes with the same software that shipped with units from two or three years ago. It doesn't make sense for Apple to release its own tablet when it knows the market is so minimal and that notebooks are getting smaller and smaller. And as everyone in the tech industry knows, Apple never announces forthcoming products anyway. Forwarding an e-mail has rewards of some kind Not even Google Gmail can track the people who forward e-mails -- it would require too much computing power and it's an invasion of privacy. So why do we still do it? (Click on image for more information about this myth.) I get forwarded e-mails almost every day. "Pass this on to save the whales," says one. "Send this to 100 people you know and win \$100," says another. Despite the rather obvious fact that no ISP could ever track e-mail forwarding from one user to another (partly for privacy reasons, partly for the sheer magnitude of collecting the data) and the fact that e-mail does not, in a technical sense, send forwarding data to any separate company -- even Microsoft -- this myth lives on. There's a mystical nature to chain mail, but one that is not founded on any legitimate dogmas. Al Gore said he invented the Internet Al Gore was misquoted. (Click on image for more information about this myth.) Here's the most famous rumor of them all. In truth, Al Gore never said he invented the Internet. What he did say was something to the effect that he encouraged legislation that helped build the foundation of the Internet, as did many other politicians back in the day. If you have your own favorite tech myth that we missed, send a note to David Ramel and we may include it in a future compilation of reader favorites. John Brandon is a freelance writer and book author who worked as an IT manager for 10 years.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115045&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• 18140 VMware Workstation, authd privileges escalation vulnerability (Remote File Checking)

VMware Workstation 6.0.x before 6.0.3 and 5.5.x before 5.5.6 on Windows allow local users to gain privileges via an unspecified manipulation that causes the authd process to connect to an arbitrary named pipe.

The issue is fixed in VMware Workstation 5.5.6 and 6.0.3.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* BUGTRAQ: 20080318 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues
<http://www.securityfocus.com/archive/1/archive/1/489739/100/0/threaded>

* MLIST: [security-announce] 20080317 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues
<http://lists.vmware.com/pipermail/security-announce/2008/000008.html>

* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2008-0005.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: 28276
<http://www.securityfocus.com/bid/28276>

* FRSIRT: ADV-2008-0905
<http://www.frsirt.com/english/advisories/2008/0905/references>

* SECTRACK: 1019621
<http://securitytracker.com/id?1019621>

* SREASON: 3755
<http://securityreason.com/securityalert/3755>

* XF: vmware-authd-privilege-escalation(41257)
<http://xforce.iss.net/xforce/xfdb/41257>

CVE Reference:

CVE-2008-1361 (cve.mitre.org, nvd.nist.gov)

• 18141 VMware Server, authd privileges escalation vulnerability (Remote File Checking)

VMware Server 1.0.x before 1.0.5 on Windows allow local users to gain privileges via an unspecified manipulation that causes the authd process to connect to an arbitrary named pipe.

The issue is fixed in VMware Server 1.0.5.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* BUGTRAQ: 20080318 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues
<http://www.securityfocus.com/archive/1/archive/1/489739/100/0/threaded>

* MLIST: [security-announce] 20080317 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues
<http://lists.vmware.com/pipermail/security-announce/2008/000008.html>

* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2008-0005.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: 28276
<http://www.securityfocus.com/bid/28276>

* FRSIRT: ADV-2008-0905
<http://www.frsirt.com/english/advisories/2008/0905/references>

* SECTRACK: 1019621

<http://securitytracker.com/id?1019621>

* SREASON: 3755

<http://securityreason.com/securityalert/3755>

* XF: vmware-authd-privilege-escalation(41257)

<http://xforce.iss.net/xforce/xfdb/41257>

CVE Reference:

CVE-2008-1361 (cve.mitre.org, nvd.nist.gov)

• 18142 VMware Workstation, authd impersonation privileges escalation or Denial of Service vulnerability (Remote File Checking)

VMware Workstation 6.0.x before 6.0.3 and 5.5.x before 5.5.6 on Windows allow local users to gain privileges or cause a denial of service by impersonating the authd process through an unspecified use of an "insecurely created named pipe".

The issue is fixed in VMware Workstation 5.5.6 and 6.0.3.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack / Gain Root** Risk: **High**

References:

* BUGTRAQ: 20080318 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues

<http://www.securityfocus.com/archive/1/archive/1/489739/100/0/threaded>

* MLIST: [security-announce] 20080317 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues

<http://lists.vmware.com/pipermail/security-announce/2008/000008.html>

* CONFIRM:

<http://www.vmware.com/security/advisories/VMSA-2008-0005.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: 28276

<http://www.securityfocus.com/bid/28276>

* FRSIRT: ADV-2008-0905

<http://www.frsirt.com/english/advisories/2008/0905/references>

* SECTRACK: 1019621

<http://securitytracker.com/id?1019621>

* SREASON: 3755

<http://securityreason.com/securityalert/3755>

* XF: vmware-namedpipes-privilege-escalation(41259)

<http://xforce.iss.net/xforce/xfdb/41259>

CVE Reference:

CVE-2008-1362 (cve.mitre.org, nvd.nist.gov)

• 18143 VMware Server, authd impersonation privileges escalation or Denial of Service vulnerability (Remote File Checking)

VMware Server 1.0.x before 1.0.5 on Windows allow local users to gain privileges or cause a denial of service by impersonating the authd process through an unspecified use of an "insecurely created named pipe".

The issue is fixed in VMware Server 1.0.5.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack / Gain Root** Risk: **High**

References:

* BUGTRAQ: 20080318 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues

<http://www.securityfocus.com/archive/1/archive/1/489739/100/0/threaded>

* MLIST: [security-announce] 20080317 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues
<http://lists.vmware.com/pipermail/security-announce/2008/000008.html>
* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2008-0005.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: 28276
<http://www.securityfocus.com/bid/28276>
* FRSIRT: ADV-2008-0905
<http://www.frsirt.com/english/advisories/2008/0905/references>
* SECTRACK: 1019621
<http://securitytracker.com/id?1019621>
* SREASON: 3755
<http://securityreason.com/securityalert/3755>
* XF: vmware-namedpipes-privilege-escalation(41259)
<http://xforce.iss.net/xforce/xfdb/41259>

CVE Reference:

CVE-2008-1362 (cve.mitre.org, nvd.nist.gov)

• 18144 VMware Workstation, VMX process hijacking privileges escalation vulnerability (Remote File Checking)

VMware Workstation 6.0.x before 6.0.3 and 5.5.x before 5.5.6 on Windows allow local users to gain privileges via an unspecified manipulation of a config.ini file located in an Application Data folder, which can be used for "hijacking the VMX process."

The issue is fixed in VMware Workstation 5.5.6 and 6.0.3.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* BUGTRAQ: 20080318 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues
<http://www.securityfocus.com/archive/1/archive/1/489739/100/0/threaded>
* MLIST: [security-announce] 20080317 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues
<http://lists.vmware.com/pipermail/security-announce/2008/000008.html>
* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2008-0005.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: 28276
<http://www.securityfocus.com/bid/28276>
* FRSIRT: ADV-2008-0905
<http://www.frsirt.com/english/advisories/2008/0905/references>
* SECTRACK: 1019622
<http://securitytracker.com/id?1019622>

* SREASON: 3755

<http://securityreason.com/securityalert/3755>

* XF: vmware-config-privilege-escalation(41252)

<http://xforce.iss.net/xforce/xfdb/41252>

CVE Reference:

CVE-2008-1363 (cve.mitre.org, nvd.nist.gov)

• 18145 VMware Server, VMX process hijacking privileges escalation vulnerability (Remote File Checking)

VMware Server 1.0.x before 1.0.5 on Windows allow local users to gain privileges via an unspecified manipulation of a config.ini file located in an Application Data folder, which can be used for "hijacking the VMX process."

The issue is fixed in VMware Server 1.0.5.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* BUGTRAQ: 20080318 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues

<http://www.securityfocus.com/archive/1/archive/1/489739/100/0/threaded>

* MLIST: [security-announce] 20080317 VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion resolve critical security issues

<http://lists.vmware.com/pipermail/security-announce/2008/000008.html>

* CONFIRM:

<http://www.vmware.com/security/advisories/VMSA-2008-0005.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: 28276

<http://www.securityfocus.com/bid/28276>

* FRISRT: ADV-2008-0905

<http://www.frsirt.com/english/advisories/2008/0905/references>

* SECTRAK: 1019622

<http://securitytracker.com/id?1019622>

* SREASON: 3755

<http://securityreason.com/securityalert/3755>

* XF: vmware-config-privilege-escalation(41252)

<http://xforce.iss.net/xforce/xfdb/41252>

CVE Reference:

CVE-2008-1363 (cve.mitre.org, nvd.nist.gov)

• 18146 VMware Workstation, VIX API 1.1.x multiple buffer overflows vulnerabilities (Remote File Checking)

Multiple buffer overflows in VIX API 1.1.x before 1.1.4 build 93057 on VMware Workstation 5.x and 6.x allow guest OS users to execute arbitrary code on the host OS via unspecified vectors.

The issue is fixed in VMware Workstation 5.5.7 build 91707 and 6.0.4 build 93057.

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

References:

* BUGTRAQ: 20080604 VMSA-2008-0009 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Fusion, VMware Server, VMware VIX API, VMware ESX, VMware ESXi resolve critical security issues

<http://www.securityfocus.com/archive/1/archive/1/493080/100/0/threaded>

* CONFIRM:

<http://www.vmware.com/security/advisories/VMSA-2008-0009.html>

* BID: 29552
<http://www.securityfocus.com/bid/29552>
* FRSIRT: ADV-2008-1744
<http://www.frsirt.com/english/advisories/2008/1744>
* SECTRACK: 1020200
<http://securitytracker.com/id?1020200>
* SECUNIA: 30556
<http://secunia.com/advisories/30556>

CVE Reference:

CVE-2008-2100 (cve.mitre.org, nvd.nist.gov)

• **18147 VMware Server, VIX API 1.1.x multiple buffer overflows vulnerabilities (Remote File Checking)**

Multiple buffer overflows in VIX API 1.1.x before 1.1.4 build 93057 on VMware Server 1.x allow guest OS users to execute arbitrary code on the host OS via unspecified vectors.

The issue is fixed in VMware Server 1.0.6 build 91891.

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

References:

* BUGTRAQ: 20080604 VMSA-2008-0009 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Fusion, VMware Server, VMware VIX API, VMware ESX, VMware ESXi resolve critical security issues
<http://www.securityfocus.com/archive/1/archive/1/493080/100/0/threaded>
* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2008-0009.html>
* BID: 29552
<http://www.securityfocus.com/bid/29552>
* FRSIRT: ADV-2008-1744
<http://www.frsirt.com/english/advisories/2008/1744>
* SECTRACK: 1020200
<http://securitytracker.com/id?1020200>
* SECUNIA: 30556
<http://secunia.com/advisories/30556>

CVE Reference:

CVE-2008-2100 (cve.mitre.org, nvd.nist.gov)

• **18148 VMware Workstation, vmware-authd untrusted search path vulnerability (Remote File Checking)**

Untrusted search path vulnerability in vmware-authd in VMware Workstation 5.x before 5.5.7 build 91707 and 6.x before 6.0.4 build 93057 allows local users to gain privileges via a library path option in a configuration file.

The issue is fixed in VMware Workstation 5.5.7 build 91707 and 6.x before 6.0.4 build 93057.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* IDEFENSE: 20080604 VMware Multiple Products vmware-authd Untrusted Library Loading Vulnerability
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=713>
* BUGTRAQ: 20080604 VMSA-2008-0009 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Fusion, VMware Server, VMware VIX API, VMware ESX, VMware ESXi resolve critical security issues
<http://www.securityfocus.com/archive/1/archive/1/493080/100/0/threaded>
* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2008-0009.html>
* FRSIRT: ADV-2008-1744
<http://www.frsirt.com/english/advisories/2008/1744>
* SECTRACK: 1020198
<http://securitytracker.com/id?1020198>
* SECUNIA: 30556
<http://secunia.com/advisories/30556>
* XF: vmware-vmwareauthd-privilege-escalation(42878)
<http://xforce.iss.net/xforce/xfdb/42878>

CVE Reference:

CVE-2008-0967 (cve.mitre.org, nvd.nist.gov)

• 18149 VMware Server, vmware-authd untrusted search path vulnerability (Remote File Checking)

Untrusted search path vulnerability in vmware-authd in VMware Server before 1.0.6 build 91891 allows local users to gain privileges via a library path option in a configuration file.

The issue is fixed in VMware Server 1.0.6 build 91891.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

- * IDEFENSE: 20080604 VMware Multiple Products vmware-authd Untrusted Library Loading Vulnerability <http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=713>
- * BUGTRAQ: 20080604 VMSA-2008-0009 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Fusion, VMware Server, VMware VIX API, VMware ESX, VMware ESXi resolve critical security issues <http://www.securityfocus.com/archive/1/archive/1/493080/100/0/threaded>
- * CONFIRM: <http://www.vmware.com/security/advisories/VMSA-2008-0009.html>
- * FRSIRT: ADV-2008-1744 <http://www.frsirt.com/english/advisories/2008/1744>
- * SECTRAK: 1020198 <http://securitytracker.com/id?1020198>
- * SECUNIA: 30556 <http://secunia.com/advisories/30556>
- * XF: vmware-vmwareauthd-privilege-escalation(42878) <http://xforce.iss.net/xforce/xfdb/42878>

CVE Reference:

CVE-2008-0967 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-4301 Microsoft CVSS 2.0 Score = 10.0

** DISPUTED ** A certain ActiveX control in iisext.dll in Microsoft Internet Information Services (IIS) allows remote attackers to set a password via a string argument to the SetPassword method. NOTE: this issue could not be reproduced by a reliable third party. In addition, the original researcher is unreliable. Therefore the original disclosure is probably erroneous.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

- XF: <http://xforce.iss.net/xforce/xfdb/45587>
- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496694/100/0/threaded>
- VIM: <http://www.attrition.org/pipermail/vim/2008-October/002081.html>

CVE Reference: [CVE-2008-4301](http://cve.mitre.org)

• CVE-2008-4295 Microsoft CVSS 2.0 Score = 5.4

Microsoft Windows Mobile 6.0 on HTC Wiza 200 and HTC MDA 8125 devices does not properly handle the first attempt to establish a Bluetooth connection to a peer with a long name, which allows remote attackers to cause a denial of service (device reboot) by configuring a Bluetooth device with a long hci name and (1) connecting directly to the Windows Mobile system or (2) waiting for the Windows Mobile system to scan for nearby devices.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

- MILWORM: <http://www.milw0rm.com/exploits/6582>

CVE Reference: [CVE-2008-4295](http://cve.mitre.org)

• CVE-2008-4299 Microsoft CVSS 2.0 Score = 5.0

A certain ActiveX control in the Microsoft Internet Authentication Service (IAS) Helper COM Component in iashlpr.dll allows remote attackers to cause a denial of service (browser crash) via a large integer value in the first argument to the PutProperty method. NOTE: this issue was disclosed by an unreliable researcher, so it might be incorrect.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

XF: <http://xforce.iss.net/xforce/xfdb/45556>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496695/100/0/threaded>

CVE Reference: [CVE-2008-4299](#)

• **CVE-2008-4300 Microsoft CVSS 2.0 Score = 5.0**

A certain ActiveX control in adsiiis.dll in Microsoft Internet Information Services (IIS) allows remote attackers to cause a denial of service (browser crash) via a long string in the second argument to the GetObject method. NOTE: this issue was disclosed by an unreliable researcher, so it might be incorrect.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

XF: <http://xforce.iss.net/xforce/xfdb/45584>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496696/100/0/threaded>

CVE Reference: [CVE-2008-4300](#)

• **CVE-2008-4381 Microsoft CVSS 2.0 Score = 5.0**

Microsoft Internet Explorer 7 allows remote attackers to cause a denial of service (application crash) via Javascript that calls the alert function with a URL-encoded string of a large number of invalid characters.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

XF: <http://xforce.iss.net/xforce/xfdb/45639>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496926/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496830/100/0/threaded>

MLIST: <http://www.openwall.com/lists/oss-security/2008/10/03/8>

MLIST: <http://www.openwall.com/lists/oss-security/2008/10/03/7>

CVE Reference: [CVE-2008-4381](#)

• **CVE-2008-4323 Microsoft CVSS 2.0 Score = 4.3**

Windows Explorer in Microsoft Windows XP SP3 allows user-assisted attackers to cause a denial of service (application crash) via a crafted .ZIP file.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

MILWORM: <http://www.milw0rm.com/exploits/6616>

CVE Reference: [CVE-2008-4323](#)

• **CVE-2008-4327 Microsoft CVSS 2.0 Score = 4.3**

gdiplus.dll in GDI+ in Microsoft Windows XP SP3 does not properly handle crafted .ico files, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a certain crash.ico file on a web site, and allows user-assisted attackers to cause a denial of service (divide-by-zero error and persistent application crash) via this crash.ico file on the desktop, a different vulnerability than CVE-2007-2237.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

BID: <http://www.securityfocus.com/bid/31432>

MILWORM: <http://www.milw0rm.com/exploits/6588>

CVE Reference: [CVE-2008-4327](#)

• **CVE-2008-3542 HP CVSS 2.0 Score = 7.8**

Unspecified vulnerability in HP Insight Diagnostics before 7.9.1.2402 allows remote attackers to read arbitrary files via unknown vectors.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

XF: <http://xforce.iss.net/xforce/xfdb/45506>

BID: <http://www.securityfocus.com/bid/31479>

HP: <http://marc.info/?l=bugtraq&m=122271894520640&w=2>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2695>

SECUNIA: <http://secunia.com/advisories/32061>

CVE Reference: [CVE-2008-3542](#)

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