VMware Player 2.5.2 Release Notes

VMware Player Version 2.5.2 | 31 March 2009 | Build 156735

Document last updated: April 13, 2009

These release notes cover the following topics:

What's New

With this release of VMware Player, certain new features and support have been added.

Support for New Guest Operating Systems

VMware provides support for the following operating systems for Player 2.5.2:

- Windows Vista Service Pack 1 and Service Pack 2
- Asianux Server 3.0 Service Pack 1
- openSUSE 11.1
- Ubuntu 8.10
- Ubuntu 8.04 LTS

VMware provides experimental support to the following operating systems for Player:

- Fedora 11
- FreeBSD 7.1
- Mandriva Linux 2009
- Novell SLE11.0
- Red Hat Enterprise Linux 5.3
- Red Hat Enterprise Linux 4.8
- Sun Solaris 10 Update 6
- Ubuntu 9.04

Prior Releases

Features from the prior releases of VMware Player are described in the following Release Notes documents:

- VMware Player 2.5.1 (http://www.vmware.com/support/player25/doc/releasenotes_player251.html) Release Notes
- VMware Player 2.5.0 (http://www.vmware.com/support/player25/doc/releasenotes_player250.html) Release Notes

Top of Page (#topofpage)

Known Issues

The known issues are grouped as follows:

Localization and Internationalization

- On Linux hosts, if you open a VMware Player 1.x or 2.0.x virtual machine that has Japanese characters in the `.vmx` file name, VMware Player 2.5 might exit unexpectedly.
- If you create a virtual machine on a host with an English locale and then try to open that virtual machine on a Japanese host where the path to the VMware Player installation directory contains certain Japanese hanzi characters or other characters that are not in the local encoding (that is, not Japanese), you might not be able to open the virtual machine.
- If a virtual machine's configuration file (`.vmx` file) contains characters outside of the ASCII character set and you want to use VMware Player 2.5 to open a virtual machine that was created with an older version of another VMware product, such as VMware Fusion 1.1, you must first open the virtual machine with a new version of that other VMware product. For example, open a Fusion 1.1 virtual machine with Fusion 2.0 and then you will be able to open it with VMware Player 2.5.

VMware Player and Virtual Machine Installation, Upgrade, and Compatibility

- On Windows hosts, attempts to upgrade from VMware Player 2.x to 2.5.x or to uninstall VMware Player 2.5.x might fail.
  Workarounds: Try to manually uninstall VMware Player a second time. On Windows Vista hosts, temporarily disable UAC and run the upgrade or uninstallation again.
- On Linux hosts that are running GL-based X server (Xgl), after you install VMware Player, you might not be able to power on a virtual machine until you reboot the host.
- If you use Avira AntiVir antivirus software on a Windows Vista host, you might have problems running virtual machines.

Smart Cards and Smart Card Readers (Experimental Support)

- On Windows XP hosts and perhaps other hosts, you might be locked out of the host if you remove a smart card from its reader in order to insert it for logging in to a virtual machine. To avoid this problem, configure the host's smart card removal behavior so that no action is taken when the smart card is removed.
- If you upgrade from VMware Player 2.0.x, or an earlier release, you might have difficulties logging in to a domain using a smart card. For example, you might see an error such as, `The system could not log you on. Your credentials could not be verified.`
- Smart cards that have been tested include ActivIdentity, Gemalto, and Oberthur, including DoD CAC type cards. Smart card readers that have been tested include:
  - Readers with USB interfaces: ActivIdentity USB V2, Gemplus USB-SW, SCM-SCR-331, HP USB Smartcard Keyboard KUS0133, Advance Card System ACR30, Litronic 215
  - Readers with serial interfaces: Gemplus American Express GCR415, SCM-SCR-131
  - Readers with PCMCIA interfaces: Omnikey CardMan 4040, SCM-SCR-243, Gemplus-PCMCIA
- Occasionally, a Linux guest might not detect the virtual smart card reader (SCR) due to guest-specific issues even after you successfully connect to the virtual SCR in the VMware Player UI. Workarounds:
  1. For all Linux guests, update the CCID driver configuration by manually adding the VMware virtual SCR vendor ID, product ID, and friendly name to the `/usr/lib/pcsc/drivers/ifd.ccid.bundle/Contents/Info.plist` file if they are not present. Add vendor ID 0x0E0F in the ifdVendorID key section, add product ID 0x0004 in the ifdProductID key section, and add **VMware Virtual Smart Card Reader** in the ifdFriendlyName key section of the `Info.plist` file.
  2. For Ubuntu 7.10 guests, use a `pcscd --hotplug` command to force a rescan of the USB bus by pcscd. This resolves a timing problem between udev and libusb in the guest.

Display

- If you use the TMS GUIMotions plug-in for Borland Delphi when writing applications that you want to run in virtual machines, the images for 3-D animation are not displayed.
- On some Linux guests, the shut down window does not appear in Unity view. If you choose **System > Quit** in an Ubuntu virtual machine while in Unity view, the shut down window does not appear. Workaround: Exit Unity view, press Tab until the desired button on the shut down window is chosen, and press Enter.
- On Linux hosts with a Linux guest, you might not be able to use Unity view to place application windows from different virtual desktops into corresponding virtual desktops on the host. Windows from different virtual desktops on the guest might all be placed in one virtual desktop on the host.
- When you place a virtual machine in Unity view, VMware Player tries to disable the guest screen saver. On some Linux guests, however, the screen saver is not disabled. If a guest's screen saver starts being used when in Unity view and if you have the guest configured to require authentication to exit the screen saver, you might get locked out of the guest. In such environments, disable the guest screen saver for any Linux virtual machine that will use Unity view often.
- Occasionally, on Windows guests, when you try to play a QuickTime video while in full screen mode, you see only a black screen.

Miscellaneous Issues

- Virtual machine streaming does not work when VMDK file is larger than 2GB
  When the virtual machine disks (VMDK) file of a virtual machine is larger than 2GB, streaming fails on the virtual machine with the following error:
  ```
  VMware Player unrecoverable error: (vmx)
  Failed to initialize streaming disks: Http I/O failure after all retry attempts (5)
  ```
  This issue is found on Workstation and Player with virtual machines running the following guest operating systems:
  - Ubuntu 8.04 32-bit
  - openSUSE 11.1
  - Windows Vista
  - RHEL 5.2 Server 64-bit

  Workaround: Convert the VMDK file to 2GB sparse or flat files. Alternatively, install a Web server that supports hosting files larger than 2GB.

- Virtual machine in root directory with virtual disk in a subdirectory does not work properly for snapshots
  If a Windows virtual machine is in root directory with virtual disk in a subdirectory, after taking a snapshot, the virtual machine cannot be powered on, cloned, cannot edit the settings, and other operations related to added virtual disk fail.
  Workaround: If a virtual machine is in a root directory, keep all its virtual disks in the same directory or move the virtual machine to a non-root directory.

- The virtual machine streaming feature is not implemented with HTTP redirects for this release.

You may also view a list of knowledge base articles (http://kb.vmware.com/enduser/std_alp.php?p_search_text=player250&p_gridsort=faqs.faq_id%3AD) related to VMware Player 2.5.

Top of Page (#topofpage)

Resolved Issues

The following issues are resolved in VMware Player 2.5.2:

Security Fixes

- **New: Host code execution vulnerability from a guest operating system**
  A critical vulnerability in the virtual machine display function might allow a guest operating system to run code on the host. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2009-1244 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1244) to this issue.

- **Windows-based host privilege escalation in hcmon.sys**
  A vulnerability in an `ioctl` function in `hcmon.sys` might be used to escalate privileges on a Windows-based host. The Common Vulnerabilities and Exposures (http://cve.mitre.org/) project has assigned the name CVE-2009-1146 to this issue.
  New releases of hosted products address a denial-of-service problem described in CVE-2008-3761, which can only be exploited by a privileged Windows account.

- **A remote denial-of-service vulnerability in authd for Windows-based hosts**
  A vulnerability in `vmware-authd.exe` could cause a denial-of-service condition on Windows hosts. The Common Vulnerabilities and Exposures (http://cve.mitre.org/) project has assigned the name CVE-2009-0177 to this issue.

- **A VMCI privilege escalation on Windows-based hosts or guests**
  Virtual Machine Communication Interface (VMCI) is an infrastructure that provides fast and efficient communication between a virtual machine and the host operating system and between two or more virtual machines on the same host. A vulnerability in `vmci.sys` might allow privilege escalation on Windows-based machines. This might occur on Windows-based hosts or inside Windows-based guest operating systems. Current versions of ESX Server do not support the VMCI interface and hence they are not affected by this vulnerability. To correct this vulnerability on Windows-based hosts, see Virtual Machine Communication Interface (VMCI) privilege escalation on Windows-based Workstation, Player, ACE and Server (http://kb.vmware.com/kb/1009826) (KB 1009826).
  The Common Vulnerabilities and Exposures (http://cve.mitre.org/) project has assigned the name CVE-2009-1147 to this issue.

- **VMnc codec heap overflow vulnerabilities**
  The VMnc codec assists in record and replay sessions. Record and replay records the dynamic virtual machine state over a period of time. Two heap overflow vulnerabilities might allow a remote attacker to execute arbitrary code on VMware hosted products. For an attack to be successful, the user must visit a malicious Web page or open a malicious video file.
  The Common Vulnerabilities and Exposures (http://cve.mitre.org/) project has assigned the names CVE-2009-0909 and CVE-2009-0910 to these issues.

Copyright © 2009 VMware, Inc. All rights reserved.