

Secure VMTools ...



[ISYS2](#) 38 posts since

Nov 26, 2007

Is there a way to prevent users from running malicious scripts via VMTools?

We use VMtools for drivers (obviously) and the Time Sync functionality. What we have discovered though is that a non-admin Windows user can make use of the VMTools Script tab to make scripts run under the System account after a reboot of the VM.

Many thanks



[Texiwill](#) 10,205 posts since

Jan 13, 2004 1. **Re: Secure VMTools** Jul 2, 2009 7:25 AM

Hello,

Moved to Security Forum.

This is unfortunate but true. Even if you were to disable VMtools by locking down who can actually run the guest daemon (which is a step you should take), anyone can access the VMware backdoor with a little coding. So your best bet is to use the VMware Hardening Guideline and set the appropriate isolation settings to disable the ability for anyone to use the VMware backdoor maliciously.

The DISA STIG Has a larger list than VMware's Hardening Guideline and my book has one that is larger than that.

Best regards,

Edward L. Haletky VMware Communities User Moderator, VMware vExpert 2009, [Virtualization Practice Analyst](#)

Now Available: ['VMware vSphere\(TM\) and Virtual Infrastructure Security: Securing the Virtual Environment'](#)

Also available ['VMWare ESX Server in the Enterprise'](#)

[SearchVMware Proj](#) | [Blue Gears](#) | [Top Virtualization Security Links](#) | [Virtualization Security Round Table Podcast](#)