

RE: More on VMWare poor guest isolation design

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-08/msg00475.html>

- *From:* Arthur Corliss <corliss@xxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 27 Aug 2007 22:49:35 -0800 (AKDT)
-

On Mon, 27 Aug 2007, M. Burnett wrote:

I should probably have already ended this discussion, but it reminds me of a discussion I had on this same list almost ten years ago trying to explain to Microsoft why a vulnerability that discloses physical paths is a big enough deal to bother patching. Their argument was that they couldn't see the risk of disclosing a physical path, and if someone could do something with that path then they could probably discover the path in the first place. My argument was that it really doesn't matter what the current risks might be, that's really not the point, let's just fix it anyway. It turns out later there were a number of IIS issues where people could execute or access files, but they needed to know the physical path first.

Dude, you're talking about apples and oranges. Path disclosure in a web app is bad, period, and should be considered a security risk. But the API you're complaining about is a *legitimate* feature with legitimate uses. Yes, it's a feature that can be very badly abused, so enabling it needs some forethought and intelligence.

I've said this once already, but it bears repeating: your concerns deserve discussion in context of vmware best practices. But I personally don't believe it merits discussion as a vulnerability. It's no more a vulnerability than, say, not setting a password on your Windows administrator account. It's obviously idiotic, but not a flaw in the software stack.

I think some of you are overanalyzing this issue. I am well aware that there are other ways to accomplish the same thing in many instances, I am not saying I have introduced a spectacular new attack vector. I would categorize this threat standing on its own as medium to low, depending on your environment. But the fact is that this thing bypasses normal OS security mechanisms and we simply cannot imagine how that might be used by an attacker in the future. Some of you keep trying to point out that owning the host always means owning the guests, but that isn't always the case, especially if you are not a full administrator on the host machine.

RE: More on VMWare poor guest isolation design

If you can use the API to spawn a process in a vm owned and operated by another user *then*, and only then, do you have a legitimate vulnerability. But you're basically complaining about being able to shoot yourself in the foot. It is still incumbent on the host admin to prevent unauthorized access, and *you* to prevent unauthorized use of your account. If those two imperatives are competently met, then vmware's functionality is of little concern.

I know that for a lot of years people have been saying that once someone can access the physical box, there's nothing more you can do. Well, that's just not true anymore. You very well can protect a physical machine and you should be able to protect a virtual guest from its host. There's no way a non-admin user is going to be able to modify the RAM of a vm. And in Windows Vista, if not already blocked, even as an administrator I would have to explicitly allow a worm to access the RAM or disk of a virtual machine. No worm is going to access a vm's resources without a UAC prompt coming up.

You've got a lot more confidence in Vista than I do. Regardless, here's the practical reality: you have an unprivileged process which can send commands to control a vm running with privileged resources, right? As someone else pointed out: why not just pause the VM (which writes the vm address space to a *user*-owned file), edit it, and restart it? I'd be very surprised if there wasn't more that could be done to a live vm as well.

Anyway you cut it, UAC is worthless in this circumstance.

The argument that owning a physical machine automatically means game over just isn't true. We should be able to say the same thing about a VM.

I'm sorry, but your expectations for the use and value of virtual machines is very much out of step with reality.

—Arthur Corliss
Live Free or Die