

Forum:[Hack Forums](#)

Thread: [VM ware hacked](#)

tretre - May 22, 2025, 1:11 pm

i see some one in other web have VM ware hacked with malwaer
so how to chack if my VM ware hacked

DramaKing - May 22, 2025, 1:23 pm

(May 22, 2025 01:11 PM)tretre Wrote: [\[CITE\]](#) i see some one in other web have VM ware hacked with malwaer

so how to chack if my VM ware hacked

Wow, there is one case of a VMware infection, and now you're worried about your system? Run an antivirus scan.

Zenthara - May 22, 2025, 4:06 pm

Are you possibly referring to the recent vulnerability found on VirtualBox? CVE-2025-30712 to be specific, in essence it allowed for an attacker to escape the confines of a Virtual Machine and have Remote Code Execution on your host machine. This however only affects [version 7.1.6 \(as noted by the Google Security Research team\)](#) and on the [National Vulnerability Database](#).

As long as you've updated your software (and I'd advise going and having a quick look) you should be fine. You can still take steps to [harden the security of your virtual environment](#) though if you're worried.

DramaKing - May 22, 2025, 5:50 pm

Just to be clear, VM escapes are only dangerous if you allow access to your VM. This is rarely a concern outside of cloud environments.

webdev77 - May 22, 2025, 5:55 pm

(May 22, 2025 05:50 PM)DramaKing Wrote: [\[CITE\]](#) Just to be clear, VM escapes are only dangerous if you allow access to your VM. This is rarely a concern outside of cloud environments.

OP is simply asking how to check their VMs for malware. That's it. Nothing to do with escapes or anything fancy.

Bastille - May 23, 2025, 3:42 am

You can start by SSHing your ESXi server and check :

- auth logs
- security logs
- commands history
- running services
- user and group lists
- open ports
- tmp folders

VMware ESXi is a Unix-like system, not exactly like Linux, so the commands might not be the same.

However if your server was compromised, you would already know (compromised / encrypted VM files with a ransomware)

