

Forum:[Hack Forums](#)

Thread: [Threat Actor Claims to Sell VMware ESXi 0-Day Exploit on Hacker Forum](#)

JoseMar - March 2, 2025, 11:54 am

Threat Actor Claims to Sell VMware ESXi 0-Day Exploit

A hacker known as “Vanger” has surfaced on underground discussion boards, claiming to sell a zero-day flaw aimed at VMware ESXi hypervisors

The flaw, which supposedly allows virtual machine escape (VME), is being sold for a steep price of \$150,000. If true, this flaw could let criminals gain access to the host system from a guest virtual machine (VM), posing a major threat to virtualized setups

It reportedly impacts VMware ESXi versions from 5. 5 to 8. 0, including certain updates like ESXi 8. 0 Update 3c and earlier editions. Vanger’s message includes specific build numbers for the affected versions, showing a detailed and deep knowledge of the VMware system

VMware 0-day Exploit Claim

The flaw allows attackers to escape the separation provided by the hypervisor, which could endanger the host operating system and other VMs on the same server

Organizations that utilize VMware products should quickly take actions to lessen possible risks:
Patch Management: Regularly update VMware ESXi hypervisors and related tools to fix known issues

Isolation: Ensure clear separation between guest VMs and hosts, limiting shared features like clipboard or folder sharing that could be abused

Monitoring: Apply strong monitoring tools to recognize unusual behavior on both guest and host systems

Access Control: Restrict administrative rights and require multi-factor authentication for accessing hypervisors

Though it is still unclear if Vanger’s exploit is real, its mere advertisement indicates that threats to virtualization technologies persist. Organizations must keep their systems current and use a layered security strategy to guard against potential VM escape attacks

Hackers continue to target critical infrastructure with advanced tactics, making proactive defensive measures more important than ever

Don’t forget to update and stay safe!

Additional sources to explore: You can also search for CVE or Title directly on Google for more information: <https://cybersecuritynews.com/threat-actor-vmware-esxi-0-day/>

Pr0m3th3us - March 5, 2025, 6:42 pm

Im curious if it actually works. Thanks for the post