

Forum:[Hack Forums](#)

Thread: [New Ransomware Attacking VMware ESXi Hosts Via SSH Tunneling](#)

JoseMar - January 23, 2025, 11:26 pm

New Ransomware Attacking VMware ESXi Hosts Via SSH Tunneling

A new wave of ransomware attacks is targeting VMware ESXi hosts through stolen credentials or vulnerability exploitation. The attackers use SSH tunneling to establish hidden SOCKS tunnels, which hide malicious traffic in legitimate administrative activity. With that, the threat actors can further proceed with lateral movement, deployment of ransomware, and encryption of virtual machine critical files-for example,.vmdk and.vm-to render systems inoperable.

With seldom-rebooted ESXi servers and mostly under-monitored, these create a perfect storm for persistent attacks. Among these, experts recommend a number of risk-reducing measures:
disabling SSH by default

prompt patching, imposing strong authentication

closely monitoring the ESXi environments to prevent such stealthy, high-impact attacks.

Source today January 24, 2025

<https://cybersecuritynews.com/ransomware-attacking-vmware-esxi-hosts/>

JoseMar - January 24, 2025, 1:18 am

(Jan 24, 2025 01:39 AM)Lowkey Wrote: [\[CITE\]](#) Are all of these preventable / patchable?

I didn't see any mention of a 0day.

Not have fixes available yet, just risk reducing measures, but patches will likely be released soon

Bastille - January 24, 2025, 1:41 am

Quote:After gathering intelligence, attackers deploy ransomware payloads to encrypt critical virtual machine files, such as .vmdk (virtual disk files) and .vmem (paging files). This renders entire virtualized environments inaccessible. A ransom demand is then issued, often accompanied by threats of data exfiltration or public disclosure.

This happened to one of our customer few years ago, and the backup VM was on the same ESXi, no external backup.

We then implemented strict policies regarding hypervisors (mostly VMware based) for all of our customers.

One of the most important option to enable is to limit the number of login attempt, to avoid bruteforcing.

Whitelisting a couple of IP addresses that are allowed to access the management of the ESXi only, and hardening these allowed machines.

SSH should definitely be disabled.

Thanks for the share !