Threat posed by new VMware hyperjacking vulnerabilities is hard to overstate



Three critical vulnerabilities in multiple virtual-machine products from VMware can give hackers unusually broad access to some of the most sensitive environments inside multiple customers' networks, the company and outside researchers warned Tuesday.

The class of attack made possible by exploiting the vulnerabilities is known under several names, including hyperjacking, hypervisor attack, or virtual machine escape. Virtual machines often run inside hosting environments to prevent one customer from being able to access or control the resources of other customers. By breaking out of one customer's isolated VM environment, a threat actor could take control of the hypervisor that apportions each VM. From there, the attacker could access the VMs of multiple customers, who often use these carefully controlled environments to host

their internal networks.

All bets off

“If you can escape to the hypervisor you can access every system,” security researcher Kevin Beaumont said on Mastodon. “If you can escape to the hypervisor, all bets are off as a boundary is broken.” He added: “With this vuln you’d be able to use it to traverse VMware managed hosting providers, private clouds orgs have built on prem etc.”

VMware warned Tuesday that it has evidence suggesting the vulnerabilities are already under active exploitation in the wild. The company didn’t elaborate. Beaumont said the vulnerabilities affect “every supported (and unsupported)” version in VMware’s ESXi, Workstation, Fusion, Cloud Foundation, and Telco Cloud Platform product lines.

https://arstechnica.com/security/2025/03/vmware-patches-3-critical-vulnerabilities-in-multiple-product-lines/