Linux Variant of REvil Ransomware Targets VMware's ESXi, NAS Devices

Subscribe to our *Threatpost Today* newsletter

Twitter

Microsoft Word also leveraged in the email campaign, which uses a 22-year-old Office RCE bug. https://t.co/pr5jq08fPx

Discussion

Some feedback on the content of this article: "MBED TLS is an implementation of the TLS and SSL protocols distributed under the Apache License. Apache is a widely used web server software that runs on the Linux platform." MBED TLS uses the Apache license, but the Apache web server software is not involved in this vulnerability. MBED TLS is commonly used by IoT and ARM devices. VMware ESXi also makes use of the MBED TLS library. VMware released patches back in March for the vulnerabilities. People who have not patched their ESXi hosts recently are the ones who should be made aware of the issue. "VMware ESXi, formerly known as ESX, is a bare metal hypervisor..." This is an incorrect comparison. It's like saying Windows 10 is formerly known at Windows 95. While they're both Windows, they're also entirely different products. ESXi is not directly derived from ESX. ESX loaded a linux kernel and then added drivers to support virtualization whereas ESXi does not use a linux kernel at all, but rather uses a proprietary VMware developed kernel. As such, a vulnerability which exploits a weakness of linux is unlikely to be able to exploit ESXi. I also wouldn't suggest a hypervisor partitions a server into VMs. A hypervisor allows multiple guest operating systems to share the physical resources of the underlying host. Partitioning typically implies dividing resources, but not sharing them. So what's really going on here is that ESXi and Linux-based NASes are being targeting, possibly leveraging vulnerabilities in the MBED TLS library. It is very much a mistake to call ESXi a linux-based system as it does not use the linux kernel. It's similar to suggesting FreeBSD is a linux distribution. Declare that on the internet at your own peril. It's ashame the article didn't suggest corrective action. "REvil is doing bad stuff, patch your NAS and ESXi hosts!"