VMWare Releases Guidance for VirtualPITA, VirtualPIE, and VirtualGATE Malware Targeting vSphere

Original release date: September 29, 2022

VMWare has released Protecting vSphere From Specialized Malware, addressing malware artifacts known as VirtualPITA (ESXi & Linux), VirtualPIE (ESXi), and VirtualGATE (Windows), which are used to exploit and gain persistent access to instances of ESXi.

CISA urges organizations employing VMWare ESXi to review the following for more information and to apply recommended mitigations and threat hunting guidance:

- VMware: Protecting vSphere From Specialized Malware
- VMware: Knowledge Base 89619 - Mitigation and Threat Hunting Guidance for Unsigned vSphere Installation Bundles (VIBs) in ESXi (including a script to audit ESXi hosts)
- VMWare: vSphere Security Configuration Guides (baseline hardening guidance for VMware vSphere)