Malware Persistence in VMWare ESXi Hypervisor

Overview

GE Gas Power is aware of a report on September 29, 2022, from researchers at Mandiant of Malware that has been deployed in VMWare ESXi hypervisor environments. The attackers used malicious vSphere installation Bundles (VIB's) to install backdoors on the ESXi hypervisors.

Further information, on November 8, 2022, VMWare released the following advisory in response to the Mandiant release.

https://www.vmware.com/security/advisories/VMSA-2022-0028.html

Severity Assessment

At this time GE Gas Power has assessed our products based on the available information to determine possible impact. Our application does not use the Community level VIB's and assess the risk to our products to be low.

Contact Information

Contact your local GE Services representative for assistance or for additional information.
For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date	Purpose
1.0	November 9, 2022	Initial release