Lodestone

AUGUST 2022

STATE OF CYBER

monthly newsletter

ESXI ON MY MIND: DEFENDING ONE OF RANSOMWARE'S NEW FAVORITE TARGETS

Ransomware groups on the rise are expanding their targets and evolving their tactics to have more devastating impacts on victims than ever. A recent trend has involved using ransomware against VMware ESXi server hosts to affect as many systems in an environment as possible, even if they are virtual machines. Defend yourself and your critical assets against these more sophisticated tactics by hardening your ESXi servers and staying abreast of the latest ransomware group strategies. Lodestone recommends that organizations with ESXi servers in their environments begin with the implementations described in the paragraphs below to equip their servers with optimized settings to better defend their businesses and critical assets.

Ensure that all ESXi servers have execInstalledOnly enabled. This requires the use of ESXCLI, a command-line interface, to change the setting. A Unified Extensible Firmware Interface (UEFI) secure boot enforcement must also be enabled. This prevents custom code from being executed within the ESXi server, including malicious code such as ransomware. Further improve upon this by setting servers to only accept executable files from installed vSphere Installation Bundles (VIBs) and always use Secure Boot protocols to block the execution of ransomware and other types of malware.

Lockdown Mode is another useful setting for strengthening the security of ESXi servers. This requires any operations to be performed through a vCenter server by default, making it more difficult for a threat actor to take control even if they have already gained some level of access to the environment. However, Lodestone understands that security must be balanced with usability for true success. Organizations should work with personnel to identify if Strict Lockdown Mode can be used, or if Normal Lockdown Mode is needed to prevent negatively impacting operations. Exception lists should also be configured for service accounts or specific users that must communicate with ESXi servers as part of their day-to-day work.

Finally, use vendor-provided resilience guidelines and security configuration guides for guidance on hardening specific versions of ESXi servers. Key guidelines include ensuring that only administrators are provisioned access to the vCenter server and ensuring that backups and restoration functionalities are working and secure. See the Worth a Read section for links to these guides and more.

SNOWBALLING RANSOMWARE VARIANTS HIGHLIGHT GROWING THREAT TO VMWARE ESXI ENVIRONMENTS

A noticeable trend has emerged in recent months of ransomware groups targeting ESXi servers, including new variant Luna and Black Basta, the topic of Lodestone's July 2022 State of Cyber newsletter. A lack of patching for the Log4j vulnerability may be a driver for this trend; Lodestone recommends patching systems in addition to reviewing security controls to harden infrastructure.

VSPHERE SECURITY

VMware regularly releases this in-depth guide for best practice security guidelines for all things vSphere, ESXi, and vCenter Server. It may be quite a read but contains invaluable wisdom on the best security controls to set your environment up for success against would-be attackers.

SECURITY CONFIGURATION GUIDES FOR VMWARE VSPHERE

Optimize security configurations with guidance tailored to the exact version of ESXi in your environment. Establish a safe environment baseline with one of these guides or strengthen existing security posture.

PRACTICAL RANSOMWARE RESILIENCE WITH VMWARE VSPHERE AND VMWARE CLOUD INFRASTRUCTURE

VMware ransomware resilience guidelines provide information on hardening vSphere and VMware Cloud infrastructure. Tips include implementing an Incident Response Plan (IRP) and hardening access to management interfaces and privileged accounts.