Lack of Antivirus Support Opens the Door to Adversaries

crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/

CrowdStrike Services - CrowdStrike Intelligence May 15, 2023

***Editor's Note**: VMware updated its knowledge base article, "Deployment of 3rd Party Agents and Anti-virus software on the ESXi Hypervisor," noting that the content is outdated and should be considered deprecated. VMware noted that the article "is expected to be updated in the future with current information."*

VMware also linked to a February 2023 blog post providing suggested guidance on reported ESXiArgs ransomware attacks and actions that concerned customers should take to protect themselves, including patching, updating out-of-date or vulnerable systems, and enforcing security hygiene best practices. In the post, VMware detailed security practices for protection of vSphere.

Since 2020, CrowdStrike has increasingly observed big game hunting (BGH) threat actors deploying Linux versions of ransomware tools specifically designed to affect VMWare's ESXi vSphere hypervisor (read Part 1 and Part 2 of this series).

In the first quarter of 2023, this trend has continued: Ransomware-as-a-service (RaaS) platforms including Alphv, Lockbit and Defray — tracked by CrowdStrike Intelligence as ALPHA SPIDER, BITWISE SPIDER and SPRITE SPIDER, respectively — have been leveraged to target ESXi. This trend is especially noteworthy given that ESXi, by design, does not support third-party agents or antivirus software and VMware states in its documentation that antivirus software is not required. This, combined with the popularity of ESXi as a widespread and popular virtualization and management system, makes the hypervisor a highly attractive target for modern adversaries.

What Is ESXi?

ESXi is a Type-1 hypervisor (aka a "bare-metal" hypervisor) developed by VMware. A hypervisor is software that runs and manages virtual machines (VMs). In contrast to Type-2 hypervisors, which run on a conventional host operating system, a Type-1 hypervisor runs directly on a dedicated host's hardware. ESXi systems are commonly managed by vCenter, a centralized server administration tool that can control multiple ESXi devices. While ESXi is not a Linux operating system, it is possible to run some Linux-compiled ELF binaries within the ESXi command shell.

Several relevant VMWare products associated with the ESXi platform include:

- **ESXi (or vSphere Hypervisor)**: acts as a server consisting of a hypervisor component, an identity and administrative component and a resource management component tied to the server's hardware
- **vCenter**: the identity and administrative component as well as a complete resource manager for a fleet of ESXi servers
- **ONE Access (or Identity Manager)**: provides single sign-on (SSO) solutions to connect to vCenter or ESXi
- **Horizon**: VMware's solution for full virtual architecture management

The State of ESXi Security

VMWare advises, *"**Antivirus software is not required with the vSphere Hypervisor and the use of such software is not supported**[1]."*

In addition to the lack of security tools for ESXi, enforced through this lack of support, several vulnerabilities are being actively exploited by threat actors. In February 2023, the French Computer Emergency Response Team (CERT-FR) reported a ransomware campaign — publicly tracked as ESXiArgs — was observed targeting internet-exposed VMware ESXi hypervisors vulnerable to CVE-2020-3992 or CVE-2021-21974.

Both vulnerabilities target the OpenSLP service in ESXi hypervisors. CVE-2021-21974 allows an unauthenticated network-adjacent adversary to execute arbitrary code on affected VMware ESXi instances, but has not been previously exploited in the wild (ITW).

CVE-2020-3992 — which has been exploited ITW — allows an unauthenticated adversary residing in the management network with access to port 427 on an ESXi machine to trigger a use-after-free issue in the OpenSLP service, resulting in remote code execution (RCE). Public reporting has also previously identified ITW CVE-2019-5544 exploitation[2], which similarly impacts the OpenSLP service and facilitates RCE on compromised systems.

In publicly reported cases of CVE-2020-3992 and CVE-2021-21974 exploitation, threat actors deployed a Python backdoor named vmtools.py to the file path /store/packages/; this filename and file path match the contents of a shell script a user on a public forum shared in relation to current ESXiArgs activity.

The Problem Is Getting Worse

VMware virtual infrastructure products are highly attractive targets for attackers due to the predominance of this vendor in the virtualization field and because VMware's product line is often a crucial component of an organization's IT infrastructure virtualization and management system.

More and more threat actors are recognizing that the lack of security tools, lack of adequate network segmentation of ESXi interfaces, and ITW vulnerabilities for ESXi create a target-rich environment. In April 2023, for example, CrowdStrike Intelligence identified a new RaaS program named MichaelKors, which provides affiliates with ransomware binaries targeting Windows and ESXi/Linux systems. Other RaaS platforms capable of targeting ESXi environments, such as Nevada ransomware, have also been launched.

In late September 2022, Mandiant researchers discovered and documented a novel malware ecosystem primarily targeting VMware ESXi and VMware vCenter servers, deployed as a malicious remote administration tool (RAT)[3]. The RAT allows for persistence on compromised servers as well as a means to interact with the underlying virtual machines and to extract sensitive information.

In late 2022, CrowdStrike Intelligence observed ALPHA SPIDER use Cobalt Strike variants to perform post-exploitation activities on ESXi servers as well as SystemBC variants to maintain persistence in networks via compromised vCenter servers. Moreover, SCATTERED SPIDER leveraged the open-source proxy tool rsocx to maintain access to victim ESXi servers.

CrowdStrike Intelligence also assesses that a myriad of named adversaries — including NEMESIS KITTEN, SILENT CHOLLIMA and eCrime actors such as PROPHET SPIDER — have used Log4Shell (CVE-2021-44228) to compromise VMware Horizon instances across a

wide range of sectors and regions.

Targeting virtual infrastructure components offers an attacker numerous advantages, including multiplying the impact of a single compromise or subverting detection and prevention mechanisms, as targeted components are often not sufficiently protected by security solutions. Because VMware products have been subject to critical vulnerabilities in the past, adversaries will likely continue to target any potential weaknesses, as successful compromises typically provide access to high-value resources.

Attack Vectors

Credential Theft

The most straightforward attack vector against an ESXi hypervisor is the theft of user credentials. Following credential theft, an adversary can simply authenticate against the server to advance the attack based on the attacker's objectives. If an attacker has sufficient privileges to enable and access the SSH console, arbitrary code can be executed directly, even on the most recent ESXi versions.

If the compromised account provides access to the VM's network management capabilities, the attacker can potentially reconfigure the VM to act as a proxy for accessing the internal network. Furthermore, if a compromised account only provides access to a set of VMs, configuration weaknesses or vulnerabilities affecting the virtualized OS can be targeted to advance into the target network.

Once an adversary with limited privileges has gained access to an ESXi server, privilege escalation is typically the essential intermediate step between initial access and reaching the actual objective. The cross-site scripting (XSS) vulnerabilities tracked as CVE-2016-7463, CVE-2017-4940 and CVE-2020-3955 can potentially be targeted as a means to trick a privileged user to execute code. CVE-2020-3955, for example, can be leveraged by first embedding a malicious payload in the VM properties (such as its hostname) and then tricking a system administrator to access these malicious properties through the VMware administrative interface. None of these XSS vulnerabilities are known to be exploited ITW. An additional privilege escalation vulnerability — CVE-2021-22043 — allows a user with access to settings to escalate privileges; however, as of this writing, proof-of-concept (POC) code or weaponized exploit code targeting this vulnerability is not publicly available. Furthermore, CrowdStrike Intelligence is not aware of ITW exploitation activity involving this specific weakness.

According to industry reporting, credential theft appears to be the primary attack vector employed by attackers targeting ESXi servers[4]. Furthermore, incidents observed by CrowdStrike Intelligence demonstrate that attackers typically gain access to a target network

by other means and then attempt to collect ESXi credentials to achieve the final objective, such as deploying ransomware; in all of these cases, the obtained credentials were sufficiently privileged to directly execute arbitrary code.

Virtual Machine Access

As outlined in the “What Is ESXi?” section, VMs can be accessed in two ways: directly, or through ESXi via the administrative interface. The description of credential theft above applies to the latter method and will not be repeated here.

If VMs can be accessed directly, the following two scenarios are possible:

- If the VM is not sufficiently segregated from the rest of the internal network, it can potentially act as a proxy for laterally moving through the network, rendering attacks on the ESXi server unnecessary.
- If an accessible, properly segregated VM is the only entry point into a network — and therefore does not allow the attacker to penetrate the network further — the attacker must directly target the ESXi hypervisor to run code at hypervisor level. The latter must be managed (i.e., there is a network path to more machines within the network from the ESXi hypervisor). In order to attack the underlying hypervisor from a VM, adversaries typically need a VM escape exploit.

There are two methods to realize VM escapes: The first is to target the virtualization component of the hypervisor, such as targeting a vulnerability affecting the hypervisor’s hardware emulation components. Such an exploit often requires kernel-level privileges on the VM, which means an additional exploit is required to target the VM. The second method is to target a vulnerability affecting the hypervisor that is reachable through the network and uses the VM to transmit malicious network packets to the hypervisor.

Of the approximately 40 vulnerabilities potentially facilitating VM escape through the virtualization component, only two — CVE-2012-1517 and CVE-2012-1516 — target a communication component between the VM and the hypervisor on older versions of ESXi (3.5 to 4.1). All other vulnerabilities target emulated devices, such as USB (CVE-2022-31705, CVE-2021-22041, CVE-2021-22040), CD-ROM (CVE-2021-22045) or SVGA (CVE-2020-3969, CVE-2020-3962).

Since version 6.5 of ESXi introduced VMX sandboxing, a potential VM-escape attack leveraging the virtualization component of ESXi involves at least three different exploits, as illustrated below:

1. The attacker compromises a VM at kernel level through a first exploit.
2. Next, the attacker targets a device within the VM through a second exploit to obtain code execution in the VMX process.
3. The attacker then performs a third exploit allowing for VMX sandbox escape.

4. Finally, the attacker might require a fourth exploit to escalate privileges on the hypervisor.

As of this writing, no publicly available POC code for such an exploit chain exists, and documentation of these types of vulnerabilities is scarce. Due to the complexity of this attack, only advanced actors — such as nation-state adversaries — likely possess the required capabilities.

How to Protect Your Cluster

Listed below are CrowdStrike's top five recommendations that organizations should implement to mitigate the success or impact of hypervisor jackpotting.

- **Avoid direct access to ESXi hosts.** Use the vSphere Client to administer ESXi hosts that are managed by a vCenter Server. Do not access managed hosts directly with the VMware Host Client, and do not change managed hosts from the Direct Console User Interface (DCUI). (Note: This is a VMware-specific recommendation.)
- **If direct access to an ESXi host is necessary, use a hardened jump server with multifactor authentication (MFA).** ESXi access should be limited to a jump server used for only administrative or privileged purposes with full auditing capabilities and MFA enabled. Network segmentation should ensure that any SSH, Web UI and API access to ESXi or vCenter all must originate from the jump server. In addition, SSH access should be disabled, and any enablement of SSH access should trigger alerts and be investigated urgently.
- **Ensure vCenter is not exposed to the internet over SSH or HTTP.** CrowdStrike has observed adversaries gaining initial access to vCenter using valid accounts or exploiting RCE vulnerabilities (e.g., CVE-2021-21985). Although these vulnerabilities have been addressed by VMware, these services should not be exposed to the internet to mitigate risk.
- **Ensure ESXi datastore volumes are regularly backed up.** Specifically, virtual machine disk images and snapshots should be backed up daily (more frequently if possible) to an offsite storage provider. During a ransomware event, security teams should have the ability to restore systems from backups, while preventing the backups themselves being encrypted.

- **If encryption is known or suspected to be in progress, and access is not possible to kill malicious processes, a potential option is to physically disconnect the storage from the ESXi host, or even cut power to the ESXi host.** Threat actors will often change the root password once they get access, potentially locking administrators out of the system. While physical disconnection of disks could potentially cause issues or loss of data not yet written to backend storage, it will stop the ransomware from continuing to encrypt VMDKs. Shutting down guest VMs will not help, as the encryption is happening on the hypervisor itself. Ransomware for ESXi will typically include capabilities to shut down guest VMs to unlock the disk files and allow encryption to proceed.

Additional ESXi security recommendations are available from VMware at https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-B39474AF-6778-499A-B8AB-E973BE6D4899.html.

Conclusion

Adversaries will likely continue to target VMware-based virtualization infrastructure. This assessment is made with high confidence based on the increased adoption of virtualization technology by organizations transferring workloads and infrastructure into cloud environments, VMware's predominance in the field of enterprise virtualization solutions, and the routine targeting of virtualization products by targeted intrusion and eCrime actors tracked by CrowdStrike Intelligence.

Additionally, CrowdStrike Intelligence observed a noticeable increase in BGH ransomware actors targeting ESXi servers in 2022. The potentially multiplied effects of an attack — facilitated by compromising infrastructure operating multiple critical VMs — further support this assessment.

Credential theft is the most straightforward attack vector for targeting infrastructure management and virtualization products. However, since VMware products have been subject to critical vulnerabilities in the past, adversaries and industry researchers will likely continue to investigate and uncover potential weaknesses in the future. This assessment is made with high confidence, as successful compromises of enterprise virtualization products typically provide access to high-value targets and therefore make vulnerabilities affecting corresponding products highly attractive assets for adversaries. Notably, VMware ESXi 6.5 and 6.7 and vSphere 6.5 and 6.7 reached end of general support on October 15, 2022 — essentially ending security updates for the affected products.[5]

Since virtualization technology is often a crucial part of an organization's IT infrastructure, it is critical to regularly apply security updates and conduct security posture reviews — even if these processes affect the availability of network services and components.

CrowdStrike Intelligence Confidence Assessment

High Confidence: Judgments are based on high-quality information from multiple sources. High confidence in the quality and quantity of source information supporting a judgment does not imply that that assessment is an absolute certainty or fact. The judgment still has a marginal probability of being inaccurate.

Moderate Confidence: Judgments are based on information that is credibly sourced and plausible, but not of sufficient quantity or corroborated sufficiently to warrant a higher level of confidence. This level of confidence is used to express that judgments carry an increased probability of being incorrect until more information is available or corroborated.

Low Confidence: Judgments are made where the credibility of the source is uncertain, the information is too fragmented or poorly corroborated enough to make solid analytic inferences, or the reliability of the source is untested. Further information is needed for corroboration of the information or to fill known intelligence gaps.

Additional Resources

- *To learn more about eCrime adversaries tracked by CrowdStrike Intelligence, visit the CrowdStrike Adversary Universe.*
- *To find out how to incorporate intelligence on threat actors into your security strategy, visit the CrowdStrike Falcon® Intelligence page.*
- *Learn about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon® Prevent to see for yourself how true next-gen AV performs against today's most sophisticated threats.*

1. https://kb.vmware.com/s/article/80768
2. https://www.bleepingcomputer.com/news/security/new-python-malware-backdoors-vmware-esxi-servers-for-remote-access/
3. https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence
4. https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
5. https://core.vmware.com/blog/reminder-vsphere-6567-end-general-support