Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

VMware ESXi's Fatal Flaw CVE-2024-37085 Opens Doors for Ransomware Havoc

Date of Publication	Admiralty Code	TA Number
August 1, 2024	A1	TA20242290

Summary

First Seen: June 25, 2024
Affected Product: VMware ESXi hypervisors
Threat Actors: Storm-0506, Storm-1175, Octo Tempest (aka Scattered Spider), and Manatee Tempest (aka Indrik Spider)
Ransomware: Akira, Black Basta, Babuk, Lockbit, and Kuiper
Impact: VMware ESXi hypervisors have been actively exploited by ransomware groups to gain elevated permissions and deploy file-encrypting malware. The CVE-2024-37085 vulnerability, an authentication bypass flaw, allows attackers to gain full administrative access to ESXi hypervisors by exploiting a domain group whose members receive such access by default without proper validation. Despite being resolved on June 25, 2024, CVE-2024-37085 has remained a critical exploit vector for adversaries like Storm-0506, Storm-1175, Octo Tempest, and Manatee Tempest.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-37085	VMware ESXi Authentication Bypass Vulnerability	VMware ESXi	☒	✓	✓

Vulnerability Details

#1 VMware ESXi hypervisors have been actively exploited by various ransomware groups to gain elevated permissions and deploy file-encrypting malware. VMware ESXi harbors an authentication bypass vulnerability, CVE-2024-37085, that can lead to privilege escalation. This flaw involves a domain group whose members are granted full administrative access to the ESXi hypervisor by default, without proper validation.

#2 CVE-2024-37085 was among several issues resolved on June 25, 2024. Threat actors like Storm-0506, Storm-1175, Octo Tempest, and Manatee Tempest have been exploiting this vulnerability in Active Directory domain-integrated VMware ESXi hypervisors to gain full administrative access and encrypt file systems in numerous attacks. These exploits have facilitated the deployment of ransomware strains such as Akira, Black Basta, Babuk, Lockbit, and Kuiper.

#3 One method involves creating an 'ESX Admins' group in Active Directory, allowing attackers to automatically grant a new user full administrative privileges on the ESXi hypervisor. This group is not built-in and does not exist by default in Active Directory.

#4 However, when ESXi hypervisors join a domain, they do not verify the group's existence, treating any members as having full administrative rights, even if the group was created by an attacker. Additionally, membership in the group is determined by name rather than by security identifier (SID).

#5 Another method entails renaming any domain group to ESX Admins and adding a user or utilizing an existing member for administrative privileges. The final method exploits the fact that assigning any other AD group for the management of ESXi does not immediately remove the privileges of ESX Admins group members on the ESXi, allowing attackers to maintain unauthorized access.

#6 The attack chain initiated by Storm-0506 against an unnamed engineering firm in North America began with a Qakbot infection, which provided initial access to the target's network. The attackers then exploited the CVE-2023-28252 vulnerability to escalate privileges. Using tools like Cobalt Strike and Pypykatz, they compromised two domain administrators and moved laterally to four domain controllers. Storm-0506 also employed brute-force RDP attacks for further movement within the network. To maintain persistence, the attackers deployed custom tools and the SystemBC implant.

#7 To evade detection, they tampered with Microsoft Defender Antivirus. A critical point in their attack was exploiting CVE-2024-37085 by creating an 'ESX Admins' group, which granted them administrative access to the ESXi hypervisors. This enabled them to deploy Black Basta ransomware via PsExec and mass encrypt virtual machines in the ESXi hypervisor environment. Earlier this year, it was observed that threat actors are using custom Linux versions of Play, Agenda, TargetCompany, and other encryptors like Eldorado to target VMware ESXi virtual machines.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-37085	VMware ESXi 8.0, VMware ESXi 7.0, VMware Cloud Foundation 5.x, VMware Cloud Foundation 4.x	cpe:2.3:o:vmware:esxi:-:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*	CWE-287

Recommendations

Update ESXi Hypervisors: Ensure that all domain-joined ESXi hypervisors are updated to the latest security patches released by VMware. Apply the latest fixed version ESXi80U3-24022510 for ESXi 8.0 and version 5.2 for VMware Cloud Foundation 5.x.

Validate and Secure the "ESX Admins" Group: Verify that the “ESX Admins” group exists in the domain and is properly hardened. Adjust settings in the ESXi hypervisor to manually deny access to this group if full admin access is unnecessary. You can disable the automatic inclusion of this group using the advanced host setting:
Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd from true to false
Config.HostAgent.plugins.vimsvc.authValidateInterval from 1440 to 90
Config.HostAgent.plugins.hostsvc.esxAdminsGroup from "ESX Admins" to ""
Consider changing the admin group to a different group within the ESXi hypervisor for added security.

Configure SIEM Alerts for Suspicious Behavior: Set up customized alerts tailored to your environment to minimize false positives and monitor for signs of compromised infrastructure. Specifically, configure alerts for ESXi hosts shutting down all virtual machines, command-line commands with phrases such as ./encryptor, sudo ./encryptor, and encryptor/vmfs/volumes, and abnormal or suspicious user logins, including first-time logins and logins from unusual accounts.

Active Directory Monitoring and Alert Configuration: Configure alerts to detect when a group is created or when a user or group is added to an AD group named 'ESX Admins,' regardless of whether it is a global, local, or universal group. Ensure effective monitoring by setting up alerts for group creation and tracking additions to the 'ESX Admins' group. Additionally, enable audit events related to group creation and modification by configuring the “Audit account management” setting in Group Policy. This will enhance oversight and security within your Active Directory (AD) environment.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement

TA0011 Command and Control	TA0040 Impact	T1021 Remote Services	T1021.001 Remote Desktop Protocol
T1083 File and Directory Discovery	T1570 Lateral Tool Transfer	T1562 Impair Defenses	T1068 Exploitation for Privilege Escalation
T1105 Ingress Tool Transfer	T1110 Brute Force	T1136.002 Domain Account	T1059 Command and Scripting Interpreter
T1098 Account Manipulation	T1078.002 Domain Accounts	T1486 Data Encrypted for Impact	T1136 Create Account

Patch Details

It is strongly advised to upgrade to the latest fixed version, ESXi80U3-24022510 for ESXi 8.0, and version 5.2 for VMware Cloud Foundation 5.x. No patch is planned for ESXi 7.0 and VMware Cloud Foundation 4.x. No patch is scheduled for ESXi 7.0 and VMware Cloud Foundation 4.x, however, VMware has provided mitigations to address flaws in these versions.

Links:
https://customerconnect.vmware.com/patch

https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html

https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html

References

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/

https://hivepro.com/threat-advisory/new-linux-variant-of-play-ransomware-targeting-vmware-esxi-systems/

https://hivepro.com/threat-advisory/eldorado-a-new-ransomware-threat-targeting-windows-and-vmware/

https://hivepro.com/threat-advisory/novel-targetcompany-ransomware-linux-variant-now-attacks-esxi/

https://hivepro.com/threat-advisory/microsoft-addresses-zero-day-and-wormable-vulnerabilities/

https://hivepro.com/threat-advisory/akira-ransomware-nets-42-million-from-250-victims/

https://hivepro.com/threat-advisory/black-basta-ransomware-impacts-over-500-organizations-worldwide/

https://hivepro.com/threat-advisory/lockbit-ransomware-evolving-tactics-and-pervasive-impact-in-2023/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

August 1, 2024 • 5:30 AM

More at www.hivepro.com