ADVISORY FOR ICM SECTORS

Ransomware operators actively exploiting VMWare ESXi hypervisor vulnerability

Original report published on: July 29, 2024[1]

Executive Summary

ESXi hypervisors are widely used in corporate networks to host virtual machines (VM) which may include critical servers. Microsoft researchers uncovered CVE-2024-37085 (CVSS 7.2 – High) vulnerability that is actively being exploited by threat actors to obtain full administrative permissions on domain-joined VMWare ESXi hypervisors for ransomware attacks. On 30 July 2024, US' Cybersecurity and Infrastructure Security Agency (CISA) added this vulnerability to its Known Exploited Vulnerability (KEV) Catalogue based on evidence of active exploitation.

Background

Ransomware operators such as BlackByte, Storm-0506, Storm-1175, Octo Tempest, and Manatee Tempest have been actively exploiting CVE-2024-37085 to obtain full administrative permissions on domain-joined VMWare ESXi hypervisors, where some of these cases have led to Akira and Black Basta ransomware deployments.

VMware ESXi hypervisors joined to an AD domain consider any member of a domain group named "ESX Admins" to have full administrative access by default. This group is not a built-in group in AD and does not exist by default. ESXi hypervisors do not validate that such a group exists when the server is joined to a domain and still treats any members of a group with this name with full administrative access, even if the group did not originally exist. Additionally, the membership in the group is determined by name and not by security identifier (SID). Microsoft observed that most exploits in the wild involve creating a group called "ESX Admins" and then adding themselves, or other users in their control, to this group.

Successful exploitation leads to full administrative access to the ESXi hypervisors, allowing threat actors to encrypt the file system of the hypervisor, which could affect the ability of the hosted servers to run and function. It also allows the threat actor to access hosted VMs and possibly to exfiltrate data or move laterally within the network.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory:
  - Create, test and validate detection rules against the threat behaviours.
  - Validate and deny/disable processes, ports and protocols that have no business need.
- Upgrade ESXi installations as soon as possible. CVE-2024-37085 has been fixed in ESXi 8.0 Update 3 and VMware Cloud Foundation 5.2. For ESXi 7.0 and VMware Cloud Foundation v4.x, a workaround is available [2].
- Validate the group "ESX Admins" exists in the domain and is hardened.

- Manually deny access by this group by changing settings in the ESXi hypervisor itself. If full admin access for the Active Directory ESX admins group is not desired, you can disable this behavior using the advanced host setting: ‘Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd’.
- Change the admin group to a different group in the ESXi hypervisor.
- Enforce multifactor authentication (MFA) on all accounts from all devices in all locations, especially highly privileged ones that can manage other domain groups.
- Keep all operating system, software, especially on public facing systems up to date.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1078.002	Valid Accounts: Domain Accounts
Persistence	T1136.002	Create Account: Domain Account
Privilege Escalation	T1484	Domain or Tenant Policy Modification
	T1098	Account Manipulation
Impact	T1486	Data Encrypted for Impact

References

1. ^ “Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption” .
2. ^ “Secure Default Settings for ESXi Active Directory integration .