مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Ransomware Threats Targeting ESXi Hypervisors

Tracking #:432316101

Date:30-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that vulnerabilities in ESXi hypervisors being exploited by ransomware operators to execute mass encryption attacks on virtual machines hosted on ESXi servers.

TECHNICAL DETAILS:

Microsoft researchers identified vulnerabilities in ESXi hypervisors being exploited by ransomware operators, particularly through the vulnerability **CVE-2024-37085**. These vulnerabilities grant unauthorized full administrative permissions, enabling threat actors to execute mass encryption attacks on virtual machines hosted on ESXi servers. Notable groups, including Storm-0506 and Black Basta, are actively exploiting these weaknesses, resulting in significant disruption and potential data breaches for organizations globally.

CVE: **CVE-2024-37085-**VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management.

Attackers have exploited this by:

- Adding users to this group via commands, granting elevated privileges.
- Encrypting file systems of hypervisors, leading to widespread impact across hosted virtual machines.

The organized efforts from different ransomware groups signify the need for immediate and coordinated actions to secure environments against these evolving threats.

RECOMMENDATIONS:

- Immediately apply the latest security updates released by VMware for all domain-joined ESXi hypervisors to mitigate the CVE-2024-37085 vulnerability.
- Enforce multi-factor authentication (MFA) for all high-privilege accounts.
- Regularly review and tighten permissions related to account management and administrative access.
- Set up advanced monitoring across networks for suspicious group changes and access attempts.
- Configure SIEM systems to analyze logs from ESXi environments, focusing on unusual administrative access patterns.
- Establish and regularly test backup and recovery plans to safeguard against ransomware encryption.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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