مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

BlackByte Ransomware Exploits VMware ESXi Flaw

Tracking #:432316206

Date:30-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that the BlackByte ransomware group is actively exploiting vulnerabilities in VMware ESXi hypervisors and utilizing various tactics to enhance their attacks.

TECHNICAL DETAILS:

The BlackByte ransomware group is actively exploiting a recently patched vulnerability (CVE-2024-37085) in VMware ESXi hypervisors, leading to increased ransomware attacks. Their tactics include utilizing vulnerable drivers to bypass security measures and employing a self-propagating ransomware encryptor.

- **Exploitation of Vulnerabilities**: BlackByte ransomware has been exploiting a recently patched vulnerability (**CVE-2024-37085**) in VMware ESXi. This authentication bypass flaw allows attackers to gain administrator access, thereby compromising virtual machines and exploiting security controls.

- **Attack Techniques**: The group utilizes tactics such as:
  - **Bypassing Security Protections**: Through vulnerable drivers (bring your own vulnerable driver - BYOVD), they disable security processes.
  - **Initial Access**: Historically, BlackByte has exploited public vulnerabilities, including ProxyShell in Microsoft Exchange Server, and now appears to have shifted toward using VPNs for access, often obtained through brute-force attacks.

- **Double Extortion**: The group utilizes a double extortion model, threatening to leak sensitive data in addition to encryption, pressuring victims into compliance.

- **Payload Characteristics**: The ransomware encrypts files with the extension "blackbytent_h." The threat actors continue to refine their tools, shifting programming languages from C# to more complex C/C++, which enhances the malware's resilience against detection.

- **Targeted Sectors**: The group has predominantly targeted critical infrastructure sectors, including financial, food, and government facilities, suggesting a focus on high-impact organizations.

INDICATORS OF COMPROMISE(IOCs):

Hashes (SHA-256)	Description
01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd	RtCore64.sys
0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5	DBUtil_2_3.sys
543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91	zamguard64.sys
31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427	gdrv.sys

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- **Patch Vulnerabilities**: Ensure that all systems, particularly VMware ESXi hypervisors, are promptly updated to mitigate risks associated with known vulnerabilities.
- **Enhance Security Controls**:
  - Implement multi-factor authentication (MFA) to secure VPN access and administrative accounts.
  - Regularly audit and monitor user accounts for suspicious activities.
- **Endpoint Detection and Response (EDR)**: Deploy comprehensive EDR solutions to detect and mitigate lateral movement and suspicious activities within the network.
- **Incident Response Plan**: Develop and routinely test an incident response plan that includes steps for ransomware recovery and communication strategies for affected stakeholders.
- **User Training**: Conduct regular training for employees to recognize phishing attempts and understand safe practices for remote access and credential management.

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://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/