IMPORTANT CYBERSECURITY NEWS: ENCRYPTHUB EXPLOITS WINDOWS ZERO-DAY TO DEPLOY RHADAMANTHYS AND STEALC MALWARE

Vairav Cyber Security News Report

Date: March 27, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A recent cybersecurity incident involving the threat actor known as EncryptHub has led to the deployment of various malware families, including the information stealers Rhadamanthys and StealC. Attackers exploited a zero-day vulnerability, CVE-2025-26633, in Microsoft Windows' Microsoft Management Console (MMC), allowing them to manipulate .msc files and the Multilingual User Interface Path (MUIPath) to download and execute malicious payloads. This exploitation has resulted in unauthorized access to sensitive data and potential operational disruptions. Security experts are advising organizations to apply the latest patches and implement preventive measures to mitigate this risk.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: EncryptHub exploited CVE-2025-26633, an improper neutralization vulnerability in Microsoft's MMC, to deliver malware payloads. By manipulating .msc files and the MUIPath, the attackers were able to download and execute malicious payloads, maintain persistence, and steal sensitive data from infected systems. This vulnerability was patched by Microsoft earlier this month as part of its Patch Tuesday update.

Identification: The attack was identified by Trend Micro researcher Aliakbar Zahravi, who analyzed the methods used by EncryptHub to exploit the MMC vulnerability. The findings were published on March 26, 2025, highlighting the attack techniques and recommending mitigation strategies.

Threat Actor: The threat actor behind this attack is known as EncryptHub, also tracked as Water Gamayun or LARVA-208. This group has been previously analyzed by cybersecurity firms PRODAFT and Outpost24.

Affected Entities/Industries: Organizations, industries and other entities using the following Windows versions are at risk:

- Windows Server 2012 R2 (Server Core installation) version below 6.3.9600.22470

- Windows Server 2012 R2 version below 6.3.9600.22470
- Windows Server 2012 (Server Core installation) version below 6.2.9200.25368
- Windows Server 2012 version below 6.2.9200.25368
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) version below 6.1.7601.27618
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 version below 6.1.7601.27618
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) version below 6.0.6003.23168
- Windows Server 2008 for x64-based Systems Service Pack 2 version below 6.0.6003.23168
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) version below 6.0.6003.23168
- Windows Server 2008 for 32-bit Systems Service Pack 2 version below 6.0.6003.23168
- Windows Server 2016 (Server Core installation) version below 10.0.14393.7876
- Windows Server 2016 version below 10.0.14393.7876
- Windows 10 Version 1607 for x64-based Systems version below 10.0.14393.7876
- Windows 10 Version 1607 for 32-bit Systems version below 10.0.14393.7876
- Windows 10 for x64-based Systems version below 10.0.10240.20947
- Windows 10 for 32-bit Systems version below 10.0.10240.20947
- Windows Server 2025 version below 10.0.26100.3476
- Windows 11 Version 24H2 for x64-based Systems version below 10.0.26100.3476
- Windows 11 Version 24H2 for ARM64-based Systems version below 10.0.26100.3476
- Windows Server 2022, 23H2 Edition (Server Core installation) version below 10.0.25398.1486
- Windows 11 Version 23H2 for x64-based Systems version below 10.0.22631.5039
- Windows 11 Version 23H2 for ARM64-based Systems version below 10.0.22631.5039
- Windows Server 2025 (Server Core installation) version below 10.0.26100.3476
- Windows 10 Version 22H2 for 32-bit Systems version below 10.0.19045.5608

- Windows 10 Version 22H2 for ARM64-based Systems version below 10.0.19045.5608
- Windows 10 Version 22H2 for x64-based Systems version below 10.0.19045.5608
- Windows 11 Version 22H2 for x64-based Systems version below 10.0.22621.5039
- Windows 11 Version 22H2 for ARM64-based Systems version below 10.0.22621.5039
- Windows 10 Version 21H2 for x64-based Systems version below 10.0.19044.5608
- Windows 10 Version 21H2 for ARM64-based Systems version below 10.0.19044.5608
- Windows 10 Version 21H2 for 32-bit Systems version below 10.0.19044.5608
- Windows Server 2022 (Server Core installation) version below 10.0.20348.3328
- Windows Server 2022 version below 10.0.20348.3328
- Windows Server 2019 (Server Core installation) version below 10.0.17763.7009
- Windows Server 2019 version below 10.0.17763.7009
- Windows 10 Version 1809 for x64-based Systems version below 10.0.17763.7009
- Windows 10 Version 1809 for 32-bit Systems version below 10.0.17763.7009

Potential Impact: The exploitation of this vulnerability poses significant risks, including:

- Unauthorized access to sensitive data.
- Operational disruptions.
- Potential for further malware deployment.
- Reputational damage to affected organizations.

Exploitation Methods: The attack techniques employed by EncryptHub include:

- Manipulating .msc files and the MUIPath to execute malicious payloads.
- Using the ExecuteShellCommand method of MMC to download and execute next-stage payloads.
- Exploiting mock trusted directories to bypass User Account Control (UAC) and drop malicious .msc files.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Apply the latest Microsoft security patches, particularly addressing CVE-2025-26633.

- Monitor systems for unusual .msc file executions and unauthorized changes to the MUIPath.

Security Best Practices

- Educate employees about the risks of downloading and installing software from untrusted sources.
- Implement robust endpoint detection and response solutions to detect and block malicious activities.

For Advanced Security Teams

- Conduct thorough audits of system configurations related to MMC and MUIPath settings.
- Develop and deploy custom detection rules to identify exploitation attempts of CVE-2025-26633.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/03/encrypthub-exploits-windows-zero-day-to.html
- https://www.trendmicro.com/en_us/research/25/c/cve-2025-26633-water-gamayun.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com