IMPORTANT CYBERSECURITY NEWS: WINDOWS NTLM HASH LEAK FLAW EXPLOITED IN PHISHING ATTACKS ON GOVERNMENTS

Vairav Cyber Security News Report

Date: April 18, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A recent Windows vulnerability (CVE-2025-24054) that exposes NT LAN Manager (NTLM) authentication hashes via malicious .library-ms files is being actively exploited in phishing campaigns targeting government entities and private companies. Attackers leverage this flaw to steal NTLM hashes, potentially leading to unauthorized access and further compromise. Although Microsoft released a patch in March 2025, exploitation began shortly thereafter, underscoring the urgency for organizations to apply updates and review their security measures.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The vulnerability involves the use of specially crafted .library-ms files that, when interacted with (e.g., opened or previewed), trigger Windows Explorer to initiate an SMB authentication request to a remote server controlled by the attacker. This process inadvertently leaks the user's NTLM hash, which can then be captured and potentially cracked to gain unauthorized access.

Identification: Researchers from Check Point observed active exploitation between March 20 and 25, 2025, indicating that threat actors began leveraging the flaw shortly after the patch's release.

Threat Actor: One IP address involved in the attacks has been previously linked to the Russian state-sponsored group APT28 (also known as "Fancy Bear"). However, this alone is insufficient for definitive attribution.

Affected Entities/Industries: Government agencies and private sector companies have been targeted. However, any entity using the following products are vulnerable:

Product	Build Numbers less than:
Windows Server 2012 R2 (Server Core installation)	6.3.9600.22470
Windows Server 2012 R2	6.3.9600.22470

Windows Server 2012 (Server Core installation)	6.2.9200.25368
Windows Server 2012	6.2.9200.25368
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	6.1.7601.27618
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	6.1.7601.27618
Windows Server 2008 R2 for x64-based Systems Service Pack 1	6.1.7601.27618
Windows Server 2008 R2 for x64-based Systems Service Pack 1	6.1.7601.27618
Windows Server 2016 (Server Core installation)	10.0.14393.7876
Windows Server 2016	10.0.14393.7876
Windows 10 Version 1607 for x64-based Systems	10.0.14393.7876
Windows 10 Version 1607 for 32-bit Systems	10.0.14393.7876
Windows 10 for x64-based Systems	10.0.10240.20947
Windows 10 for 32-bit Systems	10.0.10240.20947
Windows Server 2025	10.0.26100.3476
Windows Server 2025	10.0.26100.3403
Windows 11 Version 24H2 for x64-based Systems	10.0.26100.3476
Windows 11 Version 24H2 for x64-based Systems	10.0.26100.3403
Windows 11 Version 24H2 for ARM64-based Systems	10.0.26100.3476
Windows 11 Version 24H2 for ARM64-based Systems	10.0.26100.3403
Windows Server 2022, 23H2 Edition (Server Core installation)	10.0.25398.1486
Windows 11 Version 23H2 for x64-based Systems	10.0.22631.5039
Windows 11 Version 23H2 for ARM64-based Systems	10.0.22631.5039
Windows Server 2025 (Server Core installation)	10.0.26100.3476
Windows Server 2025 (Server Core installation)	10.0.26100.3403
Windows 10 Version 22H2 for 32-bit Systems	10.0.19045.5608
Windows 10 Version 22H2 for ARM64-based Systems	10.0.19045.5608
Windows 10 Version 22H2 for x64-based Systems	10.0.19045.5608

Windows 11 Version 22H2 for x64-based Systems	10.0.22621.5039
Windows 11 Version 22H2 for ARM64-based Systems	10.0.22621.5039
Windows 10 Version 21H2 for x64-based Systems	10.0.19044.5608
Windows 10 Version 21H2 for ARM64-based Systems	10.0.19044.5608
Windows 10 Version 21H2 for 32-bit Systems	10.0.19044.5608
Windows Server 2022 (Server Core installation)	10.0.20348.3328
Windows Server 2022 (Server Core installation)	10.0.20348.3270
Windows Server 2022	10.0.20348.3328
Windows Server 2022	10.0.20348.3270
Windows Server 2019 (Server Core installation)	10.0.17763.7009
Windows Server 2019	10.0.17763.7009
Windows 10 Version 1809 for x64-based Systems	10.0.17763.7009
Windows 10 Version 1809 for 32-bit Systems	10.0.17763.7009

Potential Impact:

- Unauthorized access to systems
- Credential compromise
- Potential for further network infiltration

Exploitation Methods:

- Phishing emails containing malicious .library-ms files
- Minimal user interaction with these files (e.g., selecting, inspecting) that doesn't require opening or executing the file.

RELATED THREAT INTELLIGENCE & IOCs

Malicious IPs

- 159.196.128[.]120
- 194.127.179[.]157

Malware Hashes (SHA256/MD5)

- 9ca72d969d7c5494a30e996324c6c0fcb72ae1ae
- 84132ae00239e15b50c1a20126000eed29388100
- 76e93c97ffdb5adb509c966bca22e12c4508dcaa
- 7dd0131dd4660be562bc869675772e58a1e3ac8e
- 5e42c6d12f6b51364b6bfb170f4306c5ce608b4f
- 054784f1a398a35e0c5242cbfa164df0c277da73
- 7a43c177a582c777e258246f0ba818f9e73a69ab

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Apply Microsoft's March 2025 security updates to patch CVE-2025-24054.
- Educate users to avoid opening or interacting with unexpected .library-ms files.

Security Best Practices

- Implement email filtering to block malicious attachments.
- Monitor network traffic for unusual SMB authentication attempts.
- Restrict the use of NTLM where possible, favoring more secure authentication protocols.

For Advanced Security Teams

- Deploy intrusion detection systems to identify exploitation attempts.
- Conduct regular security audits to identify and remediate vulnerabilities.
- Engage in threat hunting to detect potential compromises stemming from this vulnerability.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://research.checkpoint.com/2025/cve-2025-24054-ntlm-exploit-in-the-wild/
- https://www.bleepingcomputer.com/news/security/windows-ntlm-hash-leak-flaw-exploited-in-phishing-attacks-on-governments/
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-24054

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