Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

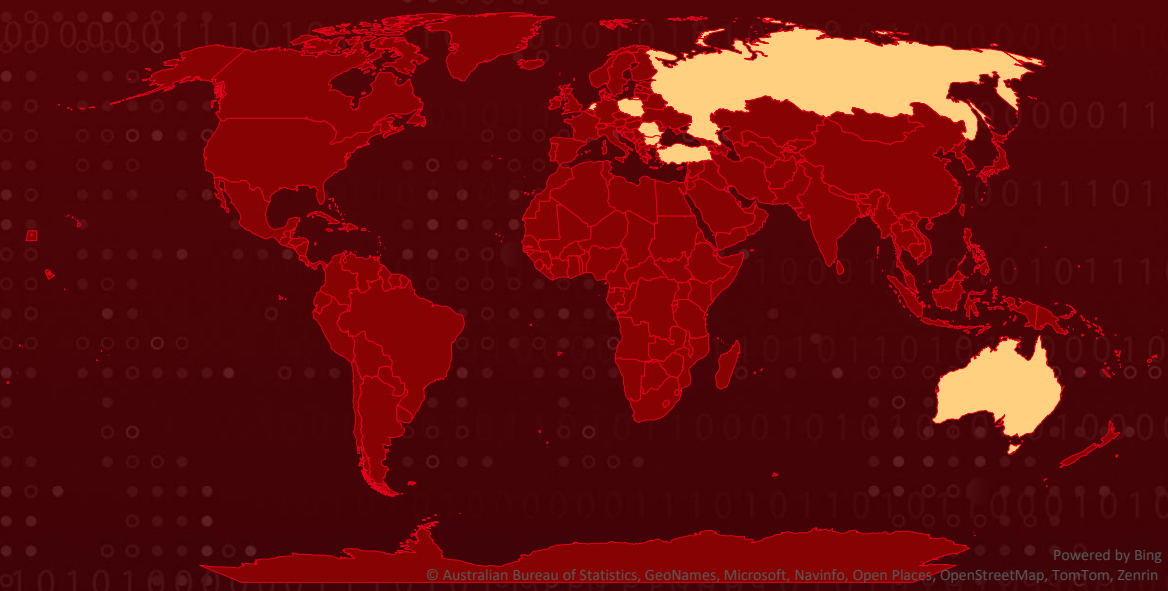
CVE-2025-24054: NTLM Hash Leak Exploit Active in the Wild

Date of Publication	Admiralty Code	TA Number
April 17, 2025	A1	TA2025119

Summary

First Seen: March 11, 2025
Affected Product: Microsoft Windows
Targeted Countries: Poland, Romania, Russia, Bulgaria, Netherlands, Australia, Turkey
Targeted Industries: Government and Private institutions
Impact: CVE-2025-24054 is a Windows vulnerability that leaks NTLMv2-SSP hashes via malicious .library-ms files with minimal user interaction. Despite a patch released on March 11, 2025, active exploitation began within days, targeting entities in Poland and Romania. Attackers used phishing emails and SMB connections to harvest credentials. The flaw poses serious risks for privilege escalation and lateral movement if left unpatched.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-24054	NTLM Hash Disclosure Spoofing Vulnerability	Microsoft Windows	✗	✓	✓
CVE-2024-43451	NTLM Hash Disclosure Spoofing Vulnerability	Microsoft Windows	✓	✓	✓

Vulnerability Details

#1

CVE-2025-24054 is a critical Windows vulnerability that enables NTLMv2-SSP hash disclosure through malicious .library-ms files. The exploit can be triggered with minimal user interaction, such as simply right-clicking, dragging and dropping, or even just navigating to a folder containing the file. Once activated, Windows Explorer initiates an SMB authentication request to a remote server, leaking the user's NTLM hash without their knowledge. Microsoft released a patch on March 11, 2025, but active exploitation in the wild began just eight days later, with several threat campaigns already leveraging the flaw to harvest credentials.

#2

The vulnerability was used in targeted malspam campaigns, notably around March 20–21, 2025, against government and private entities in Poland and Romania. Emails contained Dropbox links leading to ZIP archives with multiple exploit files, including .library-ms, .url, .website, and .lnk formats, all designed to establish SMB connections and extract NTLM hashes. The .library-ms file exploited CVE-2025-24054 directly, while the .url file referenced a previously known vulnerability, CVE-2024-43451. Both vulnerabilities allowed credential harvesting with very limited user interaction.

#3

Notably, some newer campaigns dropped the use of ZIP files altogether, instead distributing standalone .library-ms files that could trigger the exploit upon minimal contact, such as hovering over the file or viewing the containing folder. These files caused NTLMv2-SSP hashes to be transmitted to attacker-controlled SMB servers, some of which were hosted in Russia, Bulgaria, the Netherlands, and other regions. One of the IPs involved had prior ties to APT28 (Fancy Bear), though no firm attribution has been made for this specific wave of attacks.

#4

This exploitation wave underscores how rapidly threat actors adapt and weaponize newly disclosed vulnerabilities. It highlights the urgent need for organizations to apply patches promptly, disable outbound SMB where unnecessary, and enforce NTLM relay protections. Given how little user interaction is required for exploitation, CVE-2025-24054 represents a serious risk for credential theft, lateral movement, and potential domain compromise if left unaddressed.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24054	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-73
CVE-2024-43451	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-73

Recommendations

Immediate Patching: Ensure that all systems are updated with the latest Microsoft security patches, particularly the March 11, 2025 update that addresses CVE-2025-24054. Prioritize critical endpoints (e.g., servers, administrative workstations) and enforce patch compliance through centralized management tools.

Network Hardening: Enable SMB signing to prevent NTLM relay attacks. Restrict outbound SMB traffic (port 445) to internal networks only, blocking external SMB connections to attacker-controlled servers. Implement NTLM relay protections, such as Extended Protection for Authentication (EPA) or disabling NTLM where possible.

Endpoint and Email Security: Deploy endpoint detection and response (EDR) tools to identify and block malicious .library-ms files or anomalous SMB traffic. Scan incoming emails and attachments for malicious ZIP archives or phishing links, particularly those impersonating trusted services (e.g., Dropbox).

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	TA0040 Impact	TA0005 Defense Evasion	TA0002 Execution
TA0008 Lateral Movement	TA0001 Initial Access	TA0009 Collection	TA0011 Command and Control
T1566.001 Spearphishing Attachment	T1566 Phishing	T1557.001 LLMNR/NBT-NS Poisoning and SMB Relay	T1557 Adversary-in-the-Middle
T1110 Brute Force	T1550.002 Pass the Hash	T1550 Use Alternate Authentication Material	T1531 Account Access Removal
T1040 Network Sniffing	T1586 Compromise Accounts	T1102 Web Service	T1102.002 Bidirectional Communication

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	159[.]196[.]128[.]120, 194[.]127[.]179[.]157
SHA1	9ca72d969d7c5494a30e996324c6c0fcb72ae1ae, 84132ae00239e15b50c1a20126000eed29388100, 76e93c97ffdb5adb509c966bca22e12c4508dcaa, 7dd0131dd4660be562bc869675772e58a1e3ac8e, 5e42c6d12f6b51364b6bfb170f4306c5ce608b4f, 054784f1a398a35e0c5242cbfa164df0c277da73, 7a43c177a582c777e258246f0ba818f9e73a69ab

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24054

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

References

https://research.checkpoint.com/2025/cve-2025-24054-ntlm-exploit-in-the-wild/

https://hivepro.com/threat-advisory/microsofts-november-patch-tuesday-addresses-active-zero-day-exploits/

https://hivepro.com/threat-advisory/blind-eagle-cyber-reign-striking-before-you-can-blink/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

REPORT GENERATED ON

April 17, 2025 • 5:30 AM

More at www.hivepro.com