Windows Zero Day Vulnerability Exploited in the Wild

Overview

This week, a critical NTLM Hash Disclosure spoofing vulnerability (CVE-2024-43451) was found in all supported Windows versions. Exploited as a zero-day since at least April 2024, the flaw allows attackers to steal NTLMv2 hashes, allowing them to authenticate as the victim or extract their plaintext password.

CVE-2024-43451 allows attackers to steal NTLMv2 hashes from targeted systems through minimal user interaction, allowing for pass-the-hash attacks or password extraction. Threat actors have used this vulnerability in targeted campaigns, particularly against Ukrainian entities, delivering malware such as SparkRAT and Redline Infostealer.

CVE-2024-43451 can be triggered when a user interacts with a malicious URL file, such as right-clicking, deleting, or dragging it. Once exploited, it leaks the victim's NTLMv2 hash to the attacker's remote server. This allows the attacker to authenticate as the victim on the compromised system or extract the plaintext password from the hash.

Affected Products:

- Windows 7, 8, 8.1, 10, and 11
- Windows Server 2008 and later

To date, the threat actor UAC-0194 has exploited CVE-2024-43451 in a spear-phishing campaign targeting Ukrainian entities. Aspire strongly recommends applying the patch as soon as possible.

Aspire Protects

- **Patch –** Organizations should apply Microsoft's patch as soon as possible. You can find patch guidance in Microsoft's advisory.
- Disable SMB protocol for external access where feasible.
- Enable NTLM relay mitigations.
- Warn against interacting with unknown files or email links, especially URL or ZIP attachments.

IoCs

SHA-256

- aac3f49b8c875ca842f96dd6dde194102944907a956fad1ff1cff14c64aaf2e0
- 07b417ffa08f12201eceba3688690bd5c947f657be00e3c883f6ec342ec5c344
- 0efe4a603dd59b377798ae2889fe47a851f79e36d1a925d327a93416204d1767
- 6c6ba73e4c80853219121f922e60564720d414bf42d8bc542dac800560d1eb36
- df74298b2ecb33558bd34b7d59bcade5901eb5db1b61ce9aa1ae27e597f4f58d
- 928cdef8fb7c2ba9aa96ab726d74aa7a18b032102d9ec4ed00e7559f98c1bdf9

- e4a6368556c15d316960bd605827c00e336ef6e56c369090803a46ff69dfd4ac
- 715a69b898bd0a056098d24505046391e29381f671952d5e860c0cb41779a49f
- c423ea5a16e33d3b988358ad649bb43a3265cad8e118ed91863d8b9dc3e8f8f9
- caba3a8900302df5b83d260ed1f4da19b68f8c2d1b92c6dfc91b2ca01f14a1ef
- 8cf24fe1384ca8ea763081b78fd14995704bbd73a871ebe1c362053767aeec20
- 5499a4bf696fdbbe41cdc2bc9efae2df93306a135643a3651701c5ca57570eb7
- ad10aaac2661b2dd17ef586a2bf8f3dca7a82abda2580dbd3aca2d52cc5460ae
- 6de2602f486985bfadae3b4ac06af041f22fd41559954a6ecd262f7c3a8aa681
- d6d77204740bd3bdd2fd5e918a7ba9134c1d7d10eb3d6972749009dd50df6cc8
- 34073f2055002791ed3cad21be0e94b33ff4345eab8a5e7801dfdafa7cc2fb99
- e2ad6fa6dbe71e9ab10dcf3bad4b82538dabe34a3011fdaa2eeb302b67ea776d
- 6ec7f86cc19df1fef8063242ef6861355cc7ed25a669de842e1cda7332eca343
- 994fa6d6b44379a8271e0936cf2a2e898de4f720ab8c1fec98be674f20df883d

IP Addresses

- 92[.]42[.]96[.]10
- 92[.]42[.]96[.]30
- 89[.]23[.]102[.]251
- 89[.]23[.]101[.]101
- 77[.]83[.]172[.]47

TTPs to Watch

Initial Access

- Spear-phishing emails with malicious ZIP attachments (T1566.001).
- Exploit Public-Facing Application (T1190) via compromised servers.

Credential Access

- Steal Application Access Token (T1550.003) - NTLM hash disclosure.

Command and Control

- Remote Access Tool (T1219) - SparkRAT installation and execution.

Targeted Industries

- Targeted spear-phishing campaigns have already exploited this vulnerability against **educational** and **governmental** institutions in Ukraine.
- Threat actors often leverage these sectors for their access to sensitive citizen data or as staging grounds for broader attacks.

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Zero-day-cve-2024-4351-report.pdf

CVE-2024-43451 - Security Update Guide - Microsoft - NTLM Hash Disclosure Spoofing Vulnerability