Zero-Day Windows NTLM Hash Leak Vulnerability Allows for Pass-the-Hash Attacks

TL;DR

There is a vulnerability in Microsoft Windows (CVE-2026-32202, CVSS 4.3) that is being actively exploited in the wild. This vulnerability can cause a system to send NTLM authentication hashes to an attacker after a user opens a malicious file.

Attackers can use these hashes in pass-the-hash attacks to authenticate as the victim, move laterally across the network, and access sensitive data without needing the user's password.

Overview

There is a vulnerability in Microsoft Windows (CVE-2026-32202, CVSS 4.3) that stems from a protection mechanism failure in Windows Shell. The issue allows an attacker to perform spoofing and trigger NTLM hash leakage over the network.

Affected Products

This vulnerability impacts multiple Microsoft Windows versions, including:

- Windows 10 (21H2–22H2)
- Windows 11 (23H2–26H1)
- Windows Server 2012–2025

CVE-2026-32202 requires user interaction. The threat actor must deliver a malicious file, and the victim must open or execute it. When this is triggered, the system connects to the attacker's server using NTLM and sends over the user's hashed credentials.

Although the vulnerability is rated medium (4.3), it is still necessary to patch as soon as possible. CVE-2026-32202 is already being used in attacks. If an attacker gets the NTLM hash, they can log in as that user and move through the network without ever needing the password.

This vulnerability has also been added to the Known Exploited Vulnerabilities catalog by the Cybersecurity and Infrastructure Security Agency (CISA), with federal agencies required to patch by May 12, 2026.

Aspire Protects

- Apply Microsoft security updates immediately across all Windows endpoints and servers.
- Monitor for unusual NTLM authentication activity and failed logins.
- Restrict or disable NTLM authentication where possible.
- Implement SMB signing and network segmentation to limit credential relay attacks.
- Train users to avoid opening unexpected or untrusted files.

TTPs to Watch

Credential Access

- Forced Authentication [T1187] – The attacker may trigger the victim system to authenticate to a remote server, causing NTLM hashes to be exposed.

- Use Alternate Authentication Material: Pass the Hash [T1550.002] – The attacker may reuse captured NTLM hashes to authenticate as the victim without knowing the password.

Behavioral IoCs

Network Indicators

- Suspicious SMB connections to external or unknown hosts
- Outbound authentication attempts to attacker-controlled UNC paths (e.g., `\\malicious-server\share`)

Host Indicators

- Execution of unexpected or untrusted files (especially LNK or downloaded files)
- Unusual authentication activity tied to a user shortly after opening a file

Targeted Industries

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Government
- Retail

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 cyber attacks.
- **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

CVE-2026-32202 - Security Update Guide - Microsoft - Windows Shell Spoofing Vulnerability

CVE Record: CVE-2026-32202

A Shortcut to Coercion: Incomplete Patch of APT28's Zero-Day Leads to CVE-2026-32202 | Akamai