URL File NTLM Hash Disclosure Vulnerability (Zero-Day)

Overview

A newly discovered zero-day vulnerability impacts all supported and unsupported Windows Workstation and Server versions, from Windows 7 and Server 2008 R2 up to the latest Windows 11 v24H2 and Server 2022. This flaw allows attackers to capture NTLM credentials simply by tricking users into viewing a malicious file in Windows Explorer. No file execution is necessary—the vulnerability can be exploited just by opening a shared folder, USB drive, or even a Downloads folder containing a crafted file.

The issue exploits a weakness in how Windows handles outbound NTLM connections, forcing the operating system to automatically send NTLM hashes to an attacker-controlled remote share. These hashes can be cracked to reveal usernames and plaintext passwords, giving threat actors unauthorized access to accounts.

Affected Products

This vulnerability impacts:

- All versions of Windows 7, 10, 11, and their server counterparts, including legacy systems like Windows Server 2008 R2.
- Fully patched systems are not immune unless they implement additional mitigations or apply a micropatch provided by 0patch.

Although this vulnerability does not have an assigned CVE and is not currently being exploited, Aspire recommends following 0patch's guidance for patching.

Aspire Protects

- **Patch –** Apply the Free 0patch Micropatch – 0patch has released a free micropatch for affected systems. To deploy it:
  - Create a free account on 0patch Central.
  - Install the 0patch agent.
  - Allow the patch to be automatically applied.
- **Disable NTLM Authentication** – Consider turning off NTLM authentication via Group Policy:
  - Navigate to Security Settings > Local Policies > Security Options.
  - Configure the "Network Security: Restrict NTLM" policies.
  - Test the changes in a non-critical environment to avoid disruptions.

TTPs to Watch

Initial Access

- T1190 - Exploit Public-Facing Application – Forcing NTLM connections through malicious links or downloads.

Credential Access

- T1003.002 - OS Credential Dumping – NTLM Hashes – Capturing and cracking NTLM credentials.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Industries potentially affected by the URL File NTLM Hash Disclosure Vulnerability:

- Healthcare
- Education
- Retail and E-commerce
- Technology
- Retail
- Finance
- Manufacturing
- Small and Medium Sized Businesses (SMBs)

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

0patch Blog: URL File NTLM Hash Disclosure Vulnerability (0day) - and Free Micropatches for it