Windows Theme Zero-Day Vulnerability Exposes NTLM Credentials

Overview

A new zero-day vulnerability has been discovered in Windows Theme files, exposing systems to the risk of NTLM credential theft. This vulnerability is closely related to CVE-2024-38030 (CVSS 6.5), which Microsoft attempted to mitigate through a patch but remains incomplete. The flaw affects multiple versions of Windows, including the latest updates to Windows 11 (version 24H2).

This vulnerability exploits a flaw in the way Windows processes specific properties (for example, BrandImage, Wallpaper) in theme files with network file paths. When these paths are included, Windows may automatically send authenticated NTLM requests to a remote attacker-controlled host, compromising NTLM credentials without user interaction.

Microsoft's initial mitigation (PathIsUNC function) blocks network paths in theme files. However, bypass techniques from previous vulnerabilities allow attackers to evade this protection, potentially leading to unauthorized access to NTLM hashes on fully updated systems.

Affected Products

- **Windows 10 Versions** - 2004, 1909, 1809, 1803, and earlier versions
- **Windows 11 Versions** - 21H2, 22H2, 23H2, and 24H2
- **Legacy Windows Workstation Versions** - All versions up to Windows 7 with security updates applied

Although exploitation risk remains low, industries that rely heavily on email communications and file exchanges should remain cautious. Aspire recommends organizations apply the micropatch mentioned below as soon as possible.

Aspire Protects

- **Patch –** Systems can apply the 0patch micropatch to mitigate this vulnerability until an official patch is available. This micropatch is compatible with most Windows versions and is provided free for affected systems.
    - If you're new to 0patch, simply create a free account in 0patch Central and start a free trial. Next, install and register the 0patch Agent. From there, the process is fully automated—no computer reboot required. You can read the 0patch Blog post regarding CVE-2024-38030 for further details.

IoCs

- There are no known IoCs associated with the above vulnerabilities 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.

TTPs to Watch

- **Initial Access**
    - Exploit Public-Facing Application (T1190) – Attackers may craft malicious theme files and trick users into downloading and applying them to initiate NTLM credential exposure.
- **Credential Access**
    - Forced Authentication (T1078.002) – Windows sends NTLM hashes to an attacker-controlled server, allowing credential theft through forced authentication methods.

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

CVE-2024-38030 - Security Update Guide - Microsoft - Windows Themes Spoofing Vulnerability

Which Windows products has 0patch "security-adopted"? – Help Center

Recurring Windows Flaw Could Expose User Credentials

0patch Blog: We Patched CVE-2024-38030, Found Another Windows Themes Spoofing Vulnerability (0day)