Actively Exploited Zero-Day in Windows CLFS Driver

Overview

Microsoft has disclosed an actively exploited vulnerability in its Windows Common Log File System (CLFS) driver as part of its December 2024 Patch Tuesday updates. Tracked as CVE-2024-49138, this vulnerability allows attackers to escalate privileges to SYSTEM level.

CVE-2024-49138 is an elevation of privilege vulnerability with a CVSS score of 7.8. The issue affects the Windows Common Log File System (CLFS) driver and is likely caused by improper data validation within CLFS operations. Exploitation of this vulnerability requires local access, but the attack is low in complexity and does not require user interaction. Successful exploitation grants SYSTEM-level privileges, providing attackers with complete control over affected systems.

This vulnerability impacts a wide range of Windows operating systems, including:

- Windows 10 (21H2 and later)
- Windows 11 (22H2)
- Windows Server versions 2008 through 2022

CVE-2024-49138 is under active exploitation, allowing attackers to gain SYSTEM-level privileges on affected systems. Aspire recommends patching immediately.

Aspire Protects

- **Patch –** Microsoft has addressed this vulnerability with a patch. Please see Microsoft's advisory for patch guidance.
- Use advanced endpoint protection tools to detect and block malicious activities exploiting this vulnerability.

TTPs to Watch

Privilege Escalation

- Abuse Elevation Control Mechanism (T1548.002) - Exploitation of CLFS vulnerabilities to gain SYSTEM-level access.

IoCs

There are no known IoCs associated with CVE-2024-49138 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

Any organization operating on Windows infrastructure could be impacted:

- Financial Services
- Retail
- Energy
- Education
- Healthcare
- And others

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-2024-49138 - Security Update Guide - Microsoft - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2024-49138 | CVE
Microsoft fixes exploited zero-day (CVE-2024-49138) - Help Net Security