# Exploited Microsoft Zero-Day Vulnerabilities Patched

## Overview

This week, Microsoft patched two actively exploited zero-day vulnerabilities in the windows Ancillary Function Drive (AFD.sys) and in Windows Storage. These vulnerabilities could allow attackers to escalate privileges and gain system control.

CVE-2025-21418 is an elevation of privilege vulnerability in the Windows Ancillary Function Driver. This flaw is in AFD.sys, which allows Windows applications to connect to the internet. Attackers could exploit this vulnerability to execute code with SYSTEM privileges, typically in combination with a separate code execution bug. It remains unclear if the Lazarus Group, which previously exploited similar flaws, is responsible for attacks leveraging this vulnerability.

CVE-2025-21391 is an elevation of privilege vulnerability in Windows Storage. The vulnerability allows attackers to delete targeted files, potentially causing system instability or service disruption. CVE-2025-21391 could be used alongside other exploits to escalate privileges and gain full system control. This is also the first known instance of this exploitation technique being used in the wild.

Both vulnerabilities have been added to CISA's Known Exploited Vulnerabilities catalog. Aspire recommends patching immediately.

## Aspire Protects

- **Patch –** Apply Microsoft's February 2025 patches immediately.
  - Find patch guidance for CVE-2025-21418 in Microsoft's advisory.
  - Find patch guidance for CVE-2025-21391 in Microsoft's advisory.

**TTPs to Watch**

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – Attackers may exploit AFD.sys or Windows Storage flaws to gain SYSTEM privileges.

Persistence

- Rootkit [T1014] – Exploiting CVE-2025-21418 could allow attackers to install stealthy malware.

Impact

- Data Destruction [T1485] – CVE-2025-21391 may be used to delete critical files, disrupting business operations.

**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.

**Targeted Industries**

- Communications
- Government
- Energy
- Manufacturing
- Transportation
- Utilities
- Finance
- 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-2025-21418 - Security Update Guide - Microsoft - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability

CVE-2025-21391 - Security Update Guide - Microsoft - Windows Storage Elevation of Privilege Vulnerability

Zero Day Initiative — The February 2025 Security Update Review