Microsoft Fixes Two Actively Exploited Windows Zero-Days That Allow SYSTEM Access

Author: *Portia S. Cole – CTI Researcher*

TL;DR

Microsoft released security updates for two Windows zero-day vulnerabilities being used in attacks. The flaws, tracked as CVE-2026-81963 (CVSS 7.8) and CVE-2026-85880 (CVSS 7.8), allow an attacker with low-privilege local access to gain SYSTEM privileges.

Overview

There are two actively exploited privilege escalation vulnerabilities in Microsoft Windows. CVE-2026-81963 (CVSS 7.8) affects the Windows Update Stack, while CVE-2026-85880 (CVSS 7.8) affects Windows Advanced Local Procedure Call (ALPC). Microsoft has not disclosed how the vulnerabilities are being used in attacks.

Affected Products

CVE-2026-81963 affects:

- Windows 11 versions 23H2, 24H2, 25H2 and 26H1
- Windows Server 2025
- Windows Server 2025 Server Core installations

CVE-2026-85880 affects:

- Windows 10 versions 1607, 1809, 21H2 and 22H2
- Windows Server 2012 and Windows Server 2012 R2
- Windows Server 2016, 2019 and 2022
- Applicable Server Core installations

The September security release also addressed hundreds of other vulnerabilities across Windows and other Microsoft products. These include critical remote code execution flaws.

Vulnerability Breakdown

- **CVE-2026-81963 (CVSS 7.8) -** An improper link resolution vulnerability in the Windows Update Stack allows an attacker with low-privilege local access to gain SYSTEM privileges. The flaw has low attack complexity and does not require user interaction.
- **CVE-2026-85880 (CVSS 7.8) -** A heap-based buffer overflow in Windows ALPC allows code running inside a low-privilege AppContainer to escape the sandbox and gain SYSTEM privileges. No additional user interaction is required.

Published on: 9/10/2026

Neither vulnerability provides initial access. An attacker must first gain the ability to run code on the affected system.

Impact on Aspire Customers

These vulnerabilities could turn limited access to a Windows device into full control of the system. SYSTEM privileges may allow an attacker to disable security controls or access data unavailable to a standard user.

The affected products include current Windows 11 systems and older Windows servers that may still support important business applications.

The Common Vulnerability Scoring System (CVSS) rates vulnerabilities from 0 to 10 based on exploitability and potential impact.

- None (0.0): No severity
- Low (0.1–3.9): Limited impact
- Medium (4.0–6.9): Moderate risk
- High (7.0–8.9): Serious impact
- Critical (9.0–10.0): Severe impact requiring urgent attention

Aspire Protects

- **Patch** – Install the September 2026 Windows security updates on all affected systems. See Microsoft's security advisories for more information.
  - CVE-2026-85880
  - CVE-2026-81963
- Confirm that the updates were successfully installed and required restarts were completed.
- Verify that older Windows systems are covered by Extended Security Updates or upgrade them to a supported version.
- Investigate unexpected SYSTEM-level process execution that follows activity from a low-privilege application.
- Review potentially compromised devices before returning them to service. Installing an update does not remove an existing attacker.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068]: An attacker with low-privilege local access can exploit either vulnerability to gain SYSTEM privileges.

IoCs

There are no known IoCs 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 running an affected Windows version could be impacted.

- Public Sector
- Education
- Healthcare
- Finance
- Legal & Professional Services
- Retail
- Manufacturing
- Energy

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's 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.

- **NOC Services Notice**
  - If you are an Aspire NOC customer and are affected by any vulnerability in this notice, Aspire will open a case on your behalf. Customers interested in NOC services should contact Aspire's Customer Success Management team.

Supporting Documentation

CVE-2026-85880 - Security Update Guide - Microsoft - Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability

CVE-2026-81963 - Security Update Guide - Microsoft - Windows Update Stack Elevation of Privilege Vulnerability

September 2026 Security Updates - Release Notes - Security Update Guide - Microsoft