Microsoft Fixes Three Zero-Day Vulnerabilities

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Microsoft fixed three zero-day vulnerabilities in its July 2026 security updates. Two vulnerabilities affecting Active Directory Federation Services (CVE-2026-56155) and SharePoint Server (CVE-2026-56164) are being exploited, while a BitLocker vulnerability (CVE-2026-50661) was publicly disclosed before a fix was available.

Overview

There are three zero-day vulnerabilities affecting Microsoft identity, collaboration, and device-encryption products:

- CVE-2026-56155 (CVSS 7.8) is an elevation-of-privilege vulnerability in Active Directory Federation Services. An authenticated local attacker could exploit overly permissive access to the Distributed Key Manager container and gain administrator privileges. Microsoft confirmed active exploitation but did not provide details about the attacks.

- CVE-2026-56164 (CVSS 5.3) is an elevation-of-privilege vulnerability in Microsoft SharePoint Server. An unauthenticated attacker could exploit the vulnerability remotely without user interaction. The vulnerability is being actively exploited.

- CVE-2026-50661 (CVSS 6.1) is a BitLocker security feature bypass vulnerability. An attacker with physical access to a device could bypass BitLocker protection and access encrypted data. The vulnerability was publicly disclosed, but Microsoft has not seen active exploitation.

Affected Products

CVE-2026-56155:
- AD FS deployments on Windows Server 2012 and later supported versions

CVE-2026-56164:
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition

CVE-2026-50661:
- Affected Windows 10, Windows 11, and Windows Server versions listed in the Microsoft advisory

The Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2026-56155 and CVE-2026-56164 to its Known Exploited Vulnerabilities Catalog on July 14, 2026. Microsoft's July updates also address hundreds of other vulnerabilities, including critical flaws in SharePoint Server, Microsoft Defender, Windows Server Network Driver, and Active Directory Domain Services. See Microsoft's July 2026 Security Update Guide for the complete list.

Aspire Protects

- **Patch** – Apply Microsoft's July 2026 security updates to affected systems immediately. See Microsoft's advisories for more information.
  - CVE-2026-56155
  - CVE-2026-56164
  - CVE-2026-50661
- After updating AD FS servers, check the AD FS Admin event log for Event ID 1132, which indicates that the Distributed Key Manager container permissions require attention. Follow Microsoft's AD FS remediation guidance if the event appears.
- Until SharePoint updates can be installed, enable Antimalware Scan Interface protection and set Request Body Scan mode to Full.
- Review Microsoft's complete July advisory for other applicable updates.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Threat actors may exploit an internet-facing SharePoint Server to gain unauthorized access. (CVE-2026-56164)

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – Threat actors with authenticated local access may exploit the AD FS vulnerability to gain administrator privileges. (CVE-2026-56155)

Credential Access

- Unsecured Credentials: Private Keys [T1552.004] – Threat actors may obtain AD FS key material and decrypt token-signing private keys. (CVE-2026-56155)

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 using affected AD FS, SharePoint Server, or Windows systems may be impacted.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

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.

Supporting Documentation

CVE-2026-50661 - Security Update Guide - Microsoft - Windows BitLocker Security Feature Bypass Vulnerability

CVE-2026-56164 - Security Update Guide - Microsoft - Microsoft SharePoint Server Elevation of Privilege Vulnerability

CVE-2026-56155 - Security Update Guide - Microsoft - Active Directory Federation Services Elevation of Privilege Vulnerability

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