Critical Microsoft Entra ID Vulnerability Allowed Unauthenticated Remote Code Execution

Author: *Portia S. Cole – CTI Researcher*

TL;DR

There is a critical vulnerability (CVE-2026-69836, CVSS 10.0) in Microsoft Entra ID that could have allowed an unauthenticated attacker to remotely execute code without user interaction.

Microsoft fully mitigated the vulnerability within its cloud infrastructure and states that no customer action is required.

Overview

There is a critical remote code execution vulnerability in Microsoft Entra ID. The vulnerability, tracked as CVE-2026-69836 with a CVSS score of 10.0, could have allowed an unauthenticated attacker to run code remotely without user interaction. The flaw was caused by the unsafe deserialization of untrusted data.

Microsoft Entra ID is a cloud-based identity and access management service. Organizations use it to authenticate users, devices and applications, enforce access policies and control access to cloud resources. It is also used by Microsoft 365, Azure and Dynamics 365 customers.

Successful exploitation could have disrupted authentication or affected access to connected applications and business resources.

Microsoft fixed the vulnerability in its cloud environment before disclosing it, so customers do not need to take action. Microsoft initially marked the vulnerability as exploited but later corrected the advisory and confirmed that it was not exploited. No public exploit code is available.

CVE-2026-69836 affected an exclusively hosted Microsoft service. Microsoft did not identify specific customer-managed versions or on-premises products as affected.

Impact on Aspire Customers

Aspire customers may rely on Microsoft Entra ID to authenticate users, enforce access policies and control access to Microsoft 365, Azure, Dynamics 365 and other connected applications.

Successful exploitation could have allowed an attacker to execute code within Microsoft's Entra ID cloud service. This could have affected authentication services, access controls or data handled by the affected service. However, Microsoft has not

Published on: 8/24/2026

reported any exploitation or compromise of customer tenants. Microsoft fully mitigated the vulnerability, and no customer action is required.

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

- No customer action is required to remediate CVE-2026-69836. Microsoft has fully mitigated the vulnerability within the Entra ID cloud service.
- Monitor the Microsoft Security Response Center advisory for any additional revisions.
- Review Microsoft 365 Service Health notifications for any Entra ID security or availability issues affecting your organization.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] - An unauthenticated attacker may exploit the Internet-accessible Entra ID service by sending untrusted data that the service improperly deserializes, resulting in remote code execution. Microsoft states that the vulnerability was not exploited.

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

Entra ID is used across the public and private sectors, including:

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

- Retail
- Manufacturing

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 these vulnerabilities, Aspire will open a case on your behalf. Customers interested in NOC services should contact Aspire's Customer Success Management team.

Supporting Documentation

NVD - CVE-2026-69836
CVE-2026-69836 - Security Update Guide - Microsoft - Microsoft Entra ID Remote Code Execution Vulnerability