Microsoft Mitigates M365 Copilot Information Disclosure Vulnerability

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

TL;DR

A Microsoft 365 Copilot vulnerability (CVE-2026-42824) could have exposed emails, files, meeting information, password reset links, and MFA codes through a malicious Microsoft-hosted link.

An attacker could potentially access information stored in Outlook, OneDrive, SharePoint, Teams, and other Microsoft 365 services available to the affected user.

Overview

There is a vulnerability in Microsoft 365 Copilot tracked as CVE-2026-42824 (CVSS 6.5). Microsoft 365 Copilot helps users find and interact with information stored across Microsoft 365 services, including Outlook, Teams, SharePoint, OneDrive, and Exchange Online.

Affected Products

- Microsoft 365 Copilot
- Microsoft 365 Copilot Enterprise Search

The vulnerability could allow an attacker to retrieve information accessible to a signed-in Microsoft 365 user through a malicious Copilot Enterprise Search link. Information at risk includes emails, calendar entries, SharePoint documents, OneDrive files, meeting notes, password reset links, and MFA codes. Microsoft has mitigated the issue and has not observed exploitation in the wild.

Aspire Protects

- Microsoft stated that CVE-2026-42824 has been mitigated on the backend. Therefore, no customer action is required. Review Microsoft's advisory for CVE-2026-42824.
- Monitor Microsoft 365 logs for unusual Copilot Enterprise Search activity.
- Review permissions for data accessible through Microsoft Graph and Microsoft 365 Copilot.

TTPs

Collection

- Data from Information Repositories (T1213) – The vulnerability could allow access to information stored in Outlook, SharePoint, OneDrive, and other Microsoft 365 repositories.

Exfiltration

- Exfiltration Over Web Service (T1567) – Retrieved information could be transmitted to attacker-controlled infrastructure through web requests.

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 Microsoft 365 Copilot could be affected, especially those that store sensitive business information in Microsoft 365 services.

- Education
- Healthcare
- Public Sector
- Finance
- Energy
- Manufacturing
- 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 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-2026-42824 - Security Update Guide - Microsoft - M365 Copilot Information Disclosure Vulnerability