CVE-2026-24301 – Microsoft Copilot Personal One-Click Data Exfiltration Vulnerability (CoSnitch)

Severity Level: High

CVE ID - CVE-2026-24301

Components Affected

- Microsoft Copilot Personal (Consumer Edition)
- Copilot service hosted on **copilot.microsoft.com**
- Microsoft Copilot accounts authenticated using personal Microsoft accounts (MSA)

Overview

A high-severity vulnerability identified in Microsoft Copilot Personal (consumer version) could allow an attacker to execute unauthorized prompts within a victim's authenticated Copilot session through a specially crafted URL. The vulnerability, tracked as **CVE-2026-24301** and collectively referred to as **CoSnitch**, may enable the exfiltration of sensitive information from applications and services previously connected to the victim's Copilot account.

The issue was discovered by Varonis Threat Labs and reported to Microsoft in December 2025. Microsoft released security fixes on **18 August 2026**. At the time of disclosure, there was no evidence of active exploitation in the wild.

Description

The vulnerability exists in Microsoft Copilot Personal due to improper handling of URL parameters that can automatically execute prompts within a user's authenticated Copilot session.

Researchers identified an undocumented parameter, **autorun=1**, which, when combined with the existing **q** parameter, allows attacker-supplied prompts to execute automatically when a victim opens a crafted URL. The prompt executes with the same privileges and access available to the authenticated user.

The attack chain consists of:

1. Automatic execution of attacker-controlled prompts via a malicious URL.
2. Access to information available through user-authorized Copilot connectors and services.
3. Transmission of retrieved information to attacker-controlled infrastructure.
4. Persistence mechanisms through malicious memory entries created during Copilot web summarization.

An Unauthenticated Attacker May Obtain

An unauthenticated attacker who successfully convinces a victim to open a malicious Copilot URL may obtain:

- Email subject lines, message content, sender and recipient information from connected email accounts.
- Calendar event details, including titles, attendees, times, and locations.
- File names, metadata, and summaries from connected cloud storage services such as Google Drive.
- Previous Copilot conversation history.
- User-defined Copilot memory entries and saved instructions.
- Other data accessible through services previously authorized by the victim within Copilot.

The attacker does not gain permissions beyond those already granted to the victim's account but may abuse the victim's existing access to retrieve sensitive information.

Impact

Successful exploitation could result in:

- Unauthorized disclosure of sensitive personal or organizational information.
- Exposure of emails, documents, calendar information, and AI conversation history.
- Leakage of business data accessible through connected applications.
- Persistence of attacker-controlled instructions within Copilot memory.
- Increased risk of social engineering, account compromise, and data theft.
- Difficulty detecting exfiltration activity due to its similarity to legitimate Copilot operations.

Organizations using AI assistants with connected services may face increased risks because the attack leverages legitimate user permissions rather than exploiting underlying service accounts.

Solution/ Workarounds

Microsoft released security updates addressing CVE-2026-24301 on **18 August 2026**.

Organizations and users should:

1. Ensure Microsoft Copilot Personal is updated with the latest security fixes.
2. Review and remove unnecessary connected applications and third-party integrations.
3. Periodically audit Copilot memory entries and remove any suspicious or unauthorized instructions.
4. Educate users about the risks associated with opening unsolicited links related to AI assistants.
5. Monitor for unusual access patterns involving connected services and Copilot interactions.
6. Apply the principle of least privilege when authorizing applications connected to Copilot.
7. Review Microsoft security guidance and advisories related to AI assistant security.

Reference

- https://www.varonis.com/blog/cosnitch
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24301

Disclaimer

This advisory is provided for informational and defensive security purposes only. The information contained herein is based on publicly available research, vendor advisories, and responsible vulnerability disclosures available at the time of publication.