

**Computer Emergency Response Team of Mauritius**

**Ministry of Information Technology, Communication and Innovation**

**CERT-MU Security Advisory**

**CERT-MU Advisories AD-2025-02**

**Zero-Click AI Vulnerability Exposes Microsoft 365 Copilot Data Without User Interaction**

**Date of Issue:** 13 June 2025

**Severity Rating:** High

**Systems Affected:**

* Microsoft 365

**Description**

**A novel attack technique named *EchoLeak* has been characterized as a “zero-click” artificial intelligence (AI) vulnerability. This vulnerability allows attackers to exfiltrate sensitive data from Microsoft 365 (M365) Copilot’s context without any user interaction. The critical-rated vulnerability has been assigned the CVE identifier CVE-2025-32711 (CVSS score: 9.3). There is no evidence that the shortcoming was exploited maliciously in the wild.**

As a zero-click AI vulnerability, EchoLeak opens up extensive opportunities for data exfiltration and extortion attacks for motivated threat actors. In an ever-evolving agentic world, it showcases the potential risks that are inherent in the design of agents and chatbots.

**Technical details**

**As per researchers of Aim Security, an Israeli Company which discovered the vulnerability, this issue is an example of a large language model (LLM) Scope Violation that paves the way for indirect prompt injection, leading to unintended behaviour.**

**LLM Scope Violation occurs when an attacker’s instructions embedded in untrusted content, e.g., an email sent from outside an organization, successfully tricks the AI system into accessing and processing privileged internal data without explicit user intent or interaction.**

**The chains allow attackers to automatically exfiltrate sensitive and proprietary information from M365 Copilot context, without the user's awareness, or relying on any specific victim behaviour, the Israeli cybersecurity company said. The result is achieved despite M365 Copilot’s interface being open only to organization employees.**

**In EchoLeak’s case, the attacker embeds a malicious prompt payload inside markdown-formatted content, like an email, which is then parsed by the AI system's retrieval-augmented generation (RAG) engine. The payload silently triggers the LLM to extract and return private information from the user's current context.**

**The attack sequence unfolds as follows -**

* **Injection: Attacker sends an innocuous-looking email to an employee's Outlook inbox, which includes the LLM scope violation exploit**
* **User asks Microsoft 365 Copilot a business-related question (e.g., summarize and analyze their earnings report)**
* **Scope Violation: Copilot mixes untrusted attacked input with sensitive data to LLM context by the Retrieval-Augmented Generation (RAG) engine**
* **Retrieval: Copilot leaks the sensitive data to the attacker via Microsoft Teams and SharePoint URLs**

Importantly, no user clicks are required to trigger EchoLeak. The attacker relies on Copilot's default behaviour to combine and process content from Outlook and SharePoint without isolating trust boundaries – turning helpful automation into a silent leak vector.

**Solution**

**The vulnerability “EchoLeak” has been fixed by Microsoft Patch for June 2025 update. However, the increasing complexity and deeper integration of LLM applications into business workflows are already overwhelming traditional defenses. The same trend is bound to create new weaponizable flaws adversaries can stealthily exploit for high-impact attacks.**

**It is therefore advised for enterprises to:**

1. **Apply the Microsoft patch June 2025**
2. **Strengthen their prompt injection filters**
3. **Implement granular input scoping and apply post-processing filters on LLM output to block responses that contain external links or structured data.**
4. **Configure RAG engines to exclude external communications to avoid retrieving malicious prompts in the first place.**

**References**

[**https://www.aim.security/lp/aim-labs-echoleak-blogpost**](https://www.aim.security/lp/aim-labs-echoleak-blogpost)

[**https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32711**](https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32711)

**Postal address**
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation

2nd Floor, Wing A,

Shri Atal Bihari Vajpayee Tower,

Cybercity Ebene,