VULNERABILITY BULLETINS

Critical Microsoft Copilot Studio Vulnerability (CVE-2024-38206) Exposes Sensitive Data

TLP:WHITE

Aug 21, 2024

On August 20, 2024, Tenable Security published a blog post regarding a critical vulnerability affecting Microsoft Copilot Studio. Microsoft Copilot Studio is an end-to-end conversational artificial intelligence (AI) platform that enables users to create and customize copilots using natural language or a graphical interface.

The vulnerability tracked as CVE-2024-38206 is described as an information disclosure security flaw caused by a server-side request forgery (SSRF) attack. An SSRF vulnerability occurs when an attacker can influence the application to make server-side HTTP requests to unexpected targets or in an unexpected way.

Tenable security researchers exploited the vulnerability, allowing them to access Microsoft's internal infrastructure, including the Instance Metadata Service (IMDS) and internal Cosmos DB instances. Successful exploitation of these cloud services can grant access to sensitive IMDS and Cosmos DB data, including virtual machine instances and database information, respectively.

Despite Microsoft advising that no user action is required to resolve the issue, Health-ISAC provides this information to raise awareness concerning the usage of artificial intelligence as it increasingly becomes a central component across different sectors, especially healthcare.

Additional Details:

Please see the full blog post here for additional information about the critical information-disclosure vulnerability in Microsoft's Copilot Studio.

Mitigations:

As part of its Secure Future Initiative, Microsoft will require all Microsoft Azure users to have multi-factor authentication (MFA) enabled on their accounts starting October 2024. Also, Microsoft intends to enforce MFA for other Azure cloud services in early 2025.

For additional mitigation guidance, Health-ISAC recommends reviewing Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	The Hacker News, Tenable, Microsoft Blog, Dark Reading, HHS, Microsoft Blog

Release Date
Aug 22, 2024 (UTC)

Alert ID 00d68bed

View Alert

Share Feedback
was this helpful? |

Tags Copilot Studio, CVE-2024-38206, Artificial Intelligence, Microsoft

and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**