ALERTA

Vulnerabilidad Crítica en Microsoft 365 Copilot

COLCERT AL-2908-041

TLP:CLEAR

Una reciente investigación ha revelado una grave vulnerabilidad en Microsoft 365 Copilot, la herramienta de inteligencia artificial de Microsoft. Esta falla permitía a los atacantes robar información sensible de los usuarios, como correos electrónicos y documentos, a través de una cadena de explotación compleja y poco convencional.

ELEMENTOS DE INTELIGENCIA DISPONIBLES

•**Inyectar prompts maliciosos:** Introducir comandos ocultos en las solicitudes al modelo de lenguaje.

•**Automatizar tareas:** Hacer que Copilot busque y extraiga información específica de los documentos del usuario.

•**Exfiltrar datos:** Codificar la información robada en hipervínculos aparentemente inofensivos y presentárselos al usuario.

ANÁLISIS

Implicaciones y Riesgos

La explotación de esta vulnerabilidad representaba una seria amenaza para la privacidad y la seguridad de los usuarios de Microsoft 365.

Los atacantes podían acceder a información confidencial, como correos electrónicos comerciales, datos financieros y propiedad intelectual.

IMPACTO PARA COLOMBIA Y LA REGIÓN

Microsoft reconoció la gravedad de la vulnerabilidad y trabajó para solucionarla. Sin embargo, la empresa no ha divulgado los detalles específicos de la corrección, lo que dificulta evaluar la eficacia de la solución a largo plazo.

NIVEL DE RIESGO

ALTO

FUENTES:

https://www.ruetir.com/2024/08/27/microsoft-365-copilot-data-theft-vulnerability-fixed/
https://cybersecuritynews.com/copilot-prompt-injection-vulnerability/
https://www.infosecurity-magazine.com/news/microsoft-365-copilot-flaw-exposes/

COLCERT