Boletín de alerta

Boletín Nro.:
Fecha de publicación: 18/06/2026
Tema: Alerta 2026-64 Vulnerabilidad en Microsoft Copilot
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Microsoft 365 Copilot
- Microsoft 365 Copilot Enterprise Search
- Servicios hospedados de Microsoft 365 Copilot

Descripción

Microsoft publicó información de seguridad relacionada con la vulnerabilidad CVE-2026-42824, una falla de tipo Command Injection (CWE-77) que puede derivar en divulgación de información sensible dentro de entornos Microsoft 365 Copilot. La vulnerabilidad permite que un atacante no autenticado obtenga acceso a información a través de la red mediante el uso de entradas especialmente diseñadas que son procesadas por el servicio.

La vulnerabilidad fue clasificada con una puntuación CVSS v3.1 de 6.5 (Medium) con el vector:

Lo anterior indica que la explotación puede realizarse remotamente, no requiere privilegios previos, pero sí requiere interacción del usuario. El principal impacto identificado es sobre la confidencialidad de la información, sin afectar directamente la integridad o disponibilidad de los sistemas.

La descripción oficial de Microsoft indica que la vulnerabilidad se origina por una neutralización incorrecta de elementos especiales utilizados en comandos dentro de M365 Copilot, permitiendo a un atacante obtener acceso a información a través de la red.

Investigaciones adicionales han señalado que escenarios de explotación podrían permitir el acceso a información almacenada en servicios corporativos integrados con Copilot, incluyendo correos electrónicos, calendarios, documentos de SharePoint y archivos de OneDrive, dependiendo de los permisos y configuraciones existentes en el entorno afectado. Debido a que Microsoft 365 Copilot opera como un servicio en la nube estrechamente integrado con datos empresariales, una explotación exitosa podría exponer información sensible accesible por el contexto de búsqueda y los permisos del usuario afectado

Solución

Se recomiendan la siguientes acciones de forma inmediata:

- Verificar que los servicios Microsoft 365 Copilot se encuentren operando con las mitigaciones más recientes aplicadas por Microsoft.
- Revisar los permisos asignados a usuarios, grupos, SharePoint, OneDrive y otras fuentes de datos consumidas por Copilot.
- Aplicar el principio de mínimo privilegio para limitar la exposición de información sensible.

Microsoft informó que las mitigaciones fueron implementadas del lado del servicio (*server-side remediation*), por lo que normalmente no se requiere la instalación de parches por parte de los clientes. Sin embargo, se recomienda validar el estado de los servicios y revisar la exposición de datos corporativos.

Información adicional:

- **Microsoft Security Response Center – CVE-2026-42824**
- **NIST National Vulnerability Database – CVE-2026-42824**
- **Tenable CVE-2026-42824 Advisory**
- **INCIBE CVE-2026-42824 Advisory**