El pasado viernes, Microsoft dio a conocer que ha resuelto una vulnerabilidad de seguridad crítica que afectaba a Power Platform, aunque previamente recibió críticas por no actuar rápidamente al respecto.

> *«Esta vulnerabilidad podría conducir a accesos no autorizados a las funciones de Código Personalizado utilizadas en los conectores personalizados de Power Platform. El posible impacto sería la divulgación involuntaria de información si se encontraran almacenados secretos u otros datos sensibles en la función de Código Personalizado»,* declaró la empresa tecnológica.

Además, la compañía afirmó que no es necesario que los clientes tomen ninguna medida y que no encontraron evidencia de que la vulnerabilidad haya sido explotada activamente.

Tenable, quien descubrió y reportó inicialmente la deficiencia a Redmond el 30 de marzo de 2023, señaló que el problema podría permitir un acceso limitado y no autorizado a aplicaciones y datos sensibles de diferentes usuarios.

La empresa de ciberseguridad informó que el defecto surge debido a una falta de control de acceso suficiente a los hosts de Azure Function, lo que da lugar a una situación en la que un actor malintencionado podría interceptar IDs y claves secretas de clientes OAuth, así como otras formas de autenticación.

Se dice que Microsoft lanzó una solución inicial el 7 de junio de 2023, pero no fue hasta el 2 de agosto de 2023 que se corrigió completamente la vulnerabilidad.

El retraso de varios meses en parchar la falla atrajo la atención del CEO de Tenable, Amit Yoran, quien criticó duramente al fabricante de Windows por ser *«sumamente irresponsable, si no totalmente negligente».*

> *«Los proveedores de servicios en la nube han defendido durante mucho tiempo el*

> *modelo de responsabilidad compartida. Ese modelo se desmorona si tu proveedor de la nube no te notifica los problemas a medida que surgen y no implementa soluciones de manera transparente»,* dijo Yoran en una publicación compartida en LinkedIn.

> *«Lo que se escucha de Microsoft es 'solo confía en nosotros', pero lo que se recibe a cambio es muy poca transparencia y una cultura de encubrimiento perjudicial».*

La compañía tecnológica, en su propia alerta, afirmó que sigue un proceso exhaustivo de investigación e implementación de correcciones y que *«el desarrollo de una actualización de seguridad es una delicada combinación entre la velocidad y la seguridad de aplicar el parche y la calidad de la solución».*

> *«No todas las soluciones son iguales. Algunas pueden completarse y aplicarse de manera segura muy rápidamente, mientras que otras pueden llevar más tiempo. Para proteger a nuestros clientes de una explotación de una vulnerabilidad de seguridad con restricciones, también comenzamos a monitorear cualquier informe de vulnerabilidad de seguridad que esté siendo explotada activamente y actuamos con rapidez si detectamos algún ataque en curso»,* agregó la compañía