Una nueva vulnerabilidad crítica de ejecución remota de código (RCE) descubierta que afecta a múltiples servicios relacionados con Microsoft Azure, podría ser explotada por un actor malintencionado para tomar el control completo de una aplicación específica.

> *«La vulnerabilidad se logra por medio de CSRF (Falsificación de solicitud entre sitios) en el ubicuo servicio SCM Kudu. Al abusar de la vulnerabilidad, los atacantes pueden implementar archivos ZIP maliciosos que contienen una carga útil en la aplicación de Azure de la víctima»,* dijo el investigador de Ermetic, Liv Matan.

La compañía israelí de seguridad de infraestructura en la nube, que denominó la vulnerabilidad EmojiDeploy, dijo que podría permitir aún más el robo de datos confidenciales y el movimiento lateral a otros servicios de Azure.

Desde entonces, Microsoft solucionó la vulnerabilidad a partir del 6 de diciembre de 2022, después de la divulgación responsable el 26 de octubre de 2022, además de otorgar una recompensa por errores de $30,000 dólares.

Microsoft describe a Kudu como el *«motor detrás de una serie de características en Azure App Service relacionadas con la implementación basada en el control de código fuente y otros métodos de implementación como Dropbox y la sincronización de OneDrive».*

En una cadena de ataque hipotética ideada por Ermetic, un atacante podría explotar la vulnerabilidad CSRF en el panel Kudu SCM para vencer las medidas de seguridad implementadas para frustrar los ataques de origen cruzado mediante la emisión de una solicitud especialmente diseñada al punto final *«/api/zipdeploy»* para entregar un archivo malicioso (por ejemplo, web shell) y obtener el acceso remoto.

La falsificación de solicitudes entre sitios, también conocida como navegación marítima o conducción de sesiones, es un vector de ataque mediante el cual un hacker engaña a un usuario autenticado de una aplicación web para que ejecute comandos no autorizados en su nombre.

El archivo ZIP, por su parte, está codificado en el cuerpo de la solicitud HTTP, lo que hace que la aplicación de la víctima navegue a un dominio de control de actores que aloja el malware por medio de la omisión de la política del mismo origen del servidor.

> *«El impacto de la vulnerabilidad en la organización en su conjunto depende de los permisos de la identidad administrada de las aplicaciones. La aplicación efectiva del principio de privilegio mínimo puede limitar significativamente el radio de explosión»,* dijo la compañía.

Los hallazgos llegan días después de que Orca Security revelara cuatro instancias de ataques de falsificación de solicitudes del lado del servidor (SSRF) que afectaron a Azure API Management, Azure Functions, Azure Machine Learning y Azure Digital Twins.