Se ha descubierto que cuatro servicios distintos de Microsoft Azure son vulnerables a los ataques de falsificación de solicitudes del lado del servidor (SSRF) y podrían explotarse para obtener acceso no autorizado a los recursos de la nube.

Los problemas de seguridad, que fueron descubiertos por Orca entre el 8 de octubre de 2022 y el 2 de diciembre de 2022 en Azure API Management, Azure Functions, Azure Machine Learning y Azure Digital Twins, han sido abordados desde entonces por Microsoft.

> *«Las vulnerabilidades descubiertas de Azure SSRF permitieron a un atacante escanear puertos locales, encontrar nuevos servicios, puntos finales y archivos confidenciales, lo que proporcionó información valiosa sobre servidores y servicios posiblemente vulnerabilidades para explotar para la entrada inicial y la ubicación de la información confidencial»,* dijo el investigador de Orca, Lidor Ben Shitrit.

Se podría abusar de las dos vulnerabilidades que afectan a Azure Functions y Azure Digital Twins sin requerir ninguna autenticación, lo que permite a un atacante tomar el control de un servidor sin siquiera tener una cuenta de Zure en primer lugar.

Los ataques SSRF podrían tener graves consecuencias, debido a que permiten al hacker leer o actualizar los recursos internos, y además, pasar a otras partes de la red, violar sistemas que de otro modo serían inalcanzables para extraer datos valiosos.

Tres de las vulnerabilidades tienen una gravedad importante, mientras que la falla SSRF que afecta a Azure Machine Learning tiene una gravedad baja. Todas las debilidades se pueden aprovechar para manipular un servidor con el fin de montar más ataques contra un objetivo susceptible.

Las cuatro vulnerabilidades se resumen a continuación:

- SSRF no autenticado en Azure Digital Twins Explorer a través de una vulnerabilidad en el punto de conexión /proxy/blob que podría explotarse para obtener una respuesta de

cualquier servicio que tenga el sufijo *«blob.core.windows[.]net».*

- SSRF no autenticado en Azure Functions que podría explotarse para enumerar puertos locales y acceder a puntos finales internos.
- SSRF autenticado en el servicio Azure API Management, que podría explotarse para enumerar puertos internos, incluyendo uno asociado con un servicio de administración de código fuente que luego podría usarse para acceder a archivos confidenciales.
- SSRF autenticado en el servicio Azure Machine Learning a través del punto final /datacall/streamcontent que podría explotarse para obtener contenido de puntos finales arbitrarios.

Para mitigar dichas amenazas, se recomienda a las organizaciones que validen todas las entradas, se aseguren de que los servidores estén configurados para permitir solo el tráfico entrante y saliente necesario, eviten las configuraciones incorrectas y se adhieran al inicio de privilegio mínimo (PoLP).

> *«El aspecto más notable de estos descubrimientos es posiblemente la cantidad de vulnerabilidades de SSRF que pudimos encontrar con solo un esfuerzo mínimo, lo que indica qué tan frecuentes son y el riesgo que representan en entornos de nube»,* dijo Ben Shitrit.