Se revelaron dos vulnerabilidades de seguridad «peligrosas» en Microsoft Azure Bastion y Azure Container Registry, que podrían haberse aprovechado para llevar a cabo ataques de secuencias de comandos entre sitios (XSS).

> *«Las vulnerabilidades permitieron el acceso no autorizado a la sesión de la víctima dentro del iframe del servicio de Azure comprometido, lo que puede tener graves consecuencias, incluido el acceso no autorizado a los datos, las modificaciones no autorizadas y la interrupción de los iframes de los servicios de Azure»*, dijo en un comunicado el investigador de seguridad de Orca, Lidor Ben Shitrit.

Los ataques XSS tienen lugar cuando los atacantes inyectan código arbitrario en un sitio web confiable, que después se ejecuta cada vez que los usuarios incautos visitan el sitio.

Las dos vulnerabilidades identificadas por Orca aprovechan una debilidad en el iframe postMessage, que permite la comunicación de origen cruzado entre los objetivos de Windows.

Esto significaba que se podía abusar de la deficiencia para incrustar puntos finales dentro de servidores remotos usando la etiqueta iframe y, en última instancia, ejecutar código JavaScript malicioso, lo que pondría en peligro datos confidenciales.

Sin embargo, para explotar estas vulnerabilidades, un atacante tendría que realizar un reconocimiento en distintos servicios de Azure para identificar los puntos finales vulnerables integrados en el portal de Azure que pueden tener encabezados de X-Frame-Options faltantes o Políticas de Seguridad de Contenido (CSP) débiles.

> *«Una vez que el atacante incrusta exitosamente el iframe en un servidor remoto, procede a explotar el punto final mal configurado. Se enfocan en el controlador postMessage, que maneja eventos remotos como postMessages»*, dijo Ben Shitrit.

Mediante el análisis de los postMessages legítimos enviados al iframe desde portal.azure[.]com, el atacante podría posteriormente crear las cargas apropiadas mediante la incrustación del iframe vulnerable en un servidor controlado por un actor y la creación de un controlador de postMessage que entregue la carga útil maliciosa.

Por lo tanto, cuando se atrae a una víctima para que visite el punto final comprometido, la *«carga maliciosa de postMessage se entrega al iframe incrustado, lo que activa la vulnerabilidad XSS y ejecuta el código del atacante dentro del contexto de la víctima».*

Es una prueba de concepto (PoC) demostrada por Orca, se descubrió que un postMessage especialmente diseñado podía manipular el exportador SVG de vista de topología de Azure Bastion o el inicio rápido de Azure Container Registry para ejecutar una carga útil XSS.

Después de la divulgación responsable de las vulnerabilidades el 13 de abril y el 3 de mayo de 2023, Microsoft implementó correcciones de seguridad para corregirlas. No se requiere ninguna otra acción por parte de los usuarios de Azure.

La divulgación se produce más de un mes después de que Microsoft detectara tres vulnerabilidades en el servicio Azure API Management que podrían ser objeto de abuso por parte de hackers malintencionados para obtener acceso a información confidencial o servicios de back-end.