Surgieron detalles nuevos sobre una vulnerabilidad ya parcheada en Azure Service Fabric Explorer (SFX), que podría conducir a la ejecución remota de código no autenticado.

Rastreada como CVE-2023-23383 (puntaje CVSS: 8.2), la vulnerabilidad se ha denominado *«Super FabriXss»* por Orca Security, unavariante de la vulnerabilidad FabriXss (CVE-2022-35829, puntaje CVSS: 6.2) que fue corregida por Microsoft en octubre de 2022.

> *«La vulnerabilidad Super FabriXss permite a los hackers remotos aprovechar una vulnerabilidad XSS para lograr la ejecución remota de código en un contenedor alojado en un nodo de Service Fabric sin necesidad de autenticación»,* dijo el investigador de seguridad, Lidor Ben Shitrit.

XSS se refiere a un tipo de ataque de inyección de código del lado del cliente que permite cargar scripts maliciosos en sitios web confiables. Después, los scripts se ejecutan cada vez que una víctima visita el sitio web comprometido, lo que genera consecuencias no deseadas.

Aunque tanto FabriXss como Super FabriXss son vulnerabilidades de XSS, Super FabriXss tiene implicaciones más graves en el sentido de que podría usarse como arma para ejecutar código y potencialmente obtener el control de sistemas susceptibles.

Super FabriXss, que reside en la pestaña «Eventos» asociada con cada nodo en el clúster desde la interfaz de usuario, también es una vulnerabilidad XSS reflejada, lo que significa que el script está incrustado en un enlace y solo se activa cuando se hace clic en el enlace.

> *«Este ataque aprovecha las opciones de Alternar tipo de clúster en la pestaña Eventos en la plataforma Service Fabric, que permite a un atacante sobrescribir una implementación de Compose existente activando una actualización con una URL especialmente diseñada de XSS Vulnerability»,* dijo Ben Shitrit.

> *«Al tomar el control de una aplicación legítima de esta forma, el atacante puede usarla como plataforma para lanzar más ataques u obtener acceso a datos o recursos confidenciales».*

La vulnerabilidades, según Orca, afecta a Azure Service Fabric Explorer versión 9.1.1436.9590 o anterior. Desde entonces, Microsoft lo abordó como parte de su actualización del martes de parches de marzo de 2023, y la compañía lo describió como una vulnerabilidad de suplantación de identidad.

> *«La vulnerabilidad está en el cliente web, pero los scripts maliciosos ejecutados en el navegador de la víctima se traducen en acciones ejecutadas en el clúster (remoto). Un usuario víctima tendría que hacer clic en la carga útil XSS almacenada inyectada por el atacante para verse comprometida»*, dijo Microsoft en un aviso

La divulgación se produce cuando NetSPI reveló una vulnerabilidad de escalada de privilegios en Azure Function Apps, lo que permite a los usuarios con permisos de *«solo lectura»* acceder a información confidencial y obtener la ejecución de comandos.

También sigue al descubrimiento de una configuración incorrecta en Azure Active Directory que expuso una serie de aplicaciones al acceso no autorizado, incluyendo un sistema de administración de contenido (CMS) que impulsa Bing.com.

La compañía de seguridad en la nube Wiz, que nombró en código el ataque BingBang, dijo que podría usarse como arma para alterar los resultados de búsqueda en Bing, y lo que es peos, incluso realizar ataques XSS en sus usuarios.