La Agencia de Seguridad Cibernética e Infraestructura de los Estados Unidos (CISA) ha incluido una vulnerabilidad de seguridad que afecta al Servidor Microsoft SharePoint en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), basándose en pruebas de explotación activa en entornos reales.

Esta vulnerabilidad, identificada como CVE-2023-24955 (con una puntuación CVSS de 7.2), es una grave falla de ejecución remota de código que permite a un atacante autenticado con privilegios de Propietario del Sitio ejecutar código arbitrario.

> *«En un ataque basado en red, un atacante autenticado como Propietario del Sitio podría ejecutar código de manera remota en el Servidor SharePoint»,* explicó Microsoft en un aviso. Esta vulnerabilidad fue abordada por Microsoft como parte de sus actualizaciones de Patch Tuesday de mayo de 2023.

Este acontecimiento se produce más de dos meses después de que CISA añadiera CVE-2023-29357, una vulnerabilidad de escalada de privilegios en el Servidor SharePoint, a su catálogo KEV.

Es relevante destacar que en el concurso de hacking Pwn2Own Vancouver del año pasado, StarLabs SG demostró una cadena de exploits que combina CVE-2023-29357 y CVE-2023-24955, lo que les valió a los investigadores un premio de $100,000.

Sin embargo, hasta el momento no hay información sobre los ataques que estén aprovechando estas dos vulnerabilidades ni sobre los actores de amenazas que podrían estar explotándolas.

Microsoft ha indicado previamente que *«los clientes que hayan habilitado las actualizaciones automáticas y la opción de 'Recibir actualizaciones para otros productos de Microsoft' dentro de la configuración de Windows Update ya están protegidos».*

Las agencias del Poder Ejecutivo Civil Federal (FCEB) deben aplicar las correcciones antes del

16 de abril de 2024 para asegurar sus redes contra esta amenaza activa.