La Agencia de Seguridad Cibernética e Infraestructura de los Estados Unidos (CISA) ha incluido en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV) una seria vulnerabilidad de seguridad que afecta al servidor Microsoft SharePoint, respaldando su decisión con pruebas de una explotación activa.

Este problema, identificado como CVE-2023-29357 (puntuación CVSS: 9.8), consiste en una debilidad de escalada de privilegios que podría ser utilizada por un atacante para obtener privilegios de administrador. Microsoft lanzó correcciones para esta falla como parte de sus actualizaciones del martes de parches de junio de 2023.

> Según Redmond, *«Un atacante que haya adquirido acceso a tokens de autenticación JWT falsificados puede emplearlos para llevar a cabo un ataque de red que elude la autenticación y le permite obtener acceso a los privilegios de un usuario autenticado. El atacante no requiere de privilegios, ni el usuario necesita realizar ninguna acción».*

En el concurso de hacking Pwn2Own Vancouver del año pasado, el investigador de seguridad Nguyễn Tiến Giang (Jang) de StarLabs SG demostró con éxito un exploit para esta falla, logrando así ganar un premio de $100,000.

La cadena de ejecución remota preautenticada combina un bypass de autenticación (CVE-2023-29357) con un error de inyección de código (CVE-2023-24955, puntuación CVSS: 7.2), siendo este último corregido por Microsoft en mayo de 2023.

> Tiến Giang comentó en un informe técnico publicado en septiembre de 2023: *«El proceso de descubrimiento y elaboración de la cadena de exploits demandó casi un año de esfuerzo meticuloso e investigación para completarla».*

Los detalles adicionales sobre la explotación del CVE-2023-29357 en situaciones reales y la

identidad de los actores de amenazas que podrían estar aprovechándola son actualmente desconocidos. No obstante, se aconseja a las agencias federales que apliquen los parches antes del 31 de enero de 2024 para resguardarse contra esta amenaza activa.