Una falla de alta gravedad que afecta a Microsoft SharePoint ha sido incluida en el catálogo de Vulnerabilidades Explotadas Conocidas (KEV) por la Agencia de Seguridad Cibernética e Infraestructura de EE. UU. (CISA) este martes, debido a la evidencia de explotación activa.

La vulnerabilidad, identificada como CVE-2024-38094 (con una puntuación CVSS de 7.2), ha sido descrita como un fallo de deserialización que impacta a SharePoint y que podría permitir la ejecución remota de código.

> *«Un atacante autenticado con permisos de Propietario del Sitio puede aprovechar la vulnerabilidad para inyectar y ejecutar código arbitrario en el contexto del servidor de SharePoint»*, explicó Microsoft en su alerta sobre el problema.

Las actualizaciones para corregir este fallo de seguridad fueron lanzadas por Microsoft como parte de las actualizaciones de Patch Tuesday en julio de 2024. El riesgo de explotación se ve agravado por la disponibilidad pública de pruebas de concepto (PoC) que demuestran cómo explotar la vulnerabilidad.

> *«El script de prueba de concepto [...] automatiza el proceso de autenticación en un sitio de SharePoint usando NTLM, crea una carpeta y archivo específicos, y envía una carga útil XML manipulada para activar la vulnerabilidad en la API del cliente de SharePoint»,* informó SOCRadar.

Actualmente, no se han reportado casos de explotación activa del CVE-2024-38094 en entornos reales. Sin embargo, ante la posibilidad de abusos, se ha exigido a las agencias de la Rama Ejecutiva Civil Federal (FCEB) que apliquen las correcciones antes del 12 de noviembre de 2024 para proteger sus redes.

Este suceso ocurre al mismo tiempo que el Grupo de Análisis de Amenazas (TAG) de Google reveló que una vulnerabilidad de día cero recientemente parcheada en los procesadores

móviles de Samsung fue utilizada en una cadena de explotación para ejecutar código arbitrario.

Catalogada bajo el identificador CVE-2024-44068 (con una puntuación CVSS de 8.1), esta vulnerabilidad fue corregida el 7 de octubre de 2024. Samsung describió el fallo como un «*uso después de liberar en el procesador móvil que conlleva a la escalada de privilegios*».

Aunque el comunicado de Samsung no menciona si la vulnerabilidad fue explotada en la naturaleza, los investigadores de TAG de Google, Xingyu Jin y Clement Lecigne, indicaron que un exploit de día cero para esta falla se usó como parte de una cadena de escalada de privilegios.

> *«El actor puede ejecutar código arbitrario en un proceso privilegiado del 'cameraserver'. El exploit también cambió el nombre del proceso a 'vendor.samsung.hardware.camera.provider@3.0-service', probablemente para dificultar su rastreo forense»,* señalaron los investigadores.

Estas revelaciones coinciden con una nueva propuesta de CISA que presenta una serie de requisitos de seguridad para prevenir el acceso masivo a datos sensibles de EE. UU. o datos gubernamentales por parte de países o personas bajo vigilancia.

Según los nuevos requisitos, las organizaciones deben corregir vulnerabilidades explotadas conocidas dentro de 14 días, vulnerabilidades críticas sin exploits en 15 días, y vulnerabilidades graves sin exploits en 30 días.

> *«Para asegurar y verificar que un sistema restringe el acceso a los datos protegidos por parte de personas bajo vigilancia, es necesario mantener registros de auditoría de dichos accesos y tener procesos organizacionales que utilicen estos registros»,* dijo la agencia.

> *«Asimismo, es esencial que las organizaciones desarrollen sistemas de gestión de identidad para identificar qué personas tienen acceso a los diferentes conjuntos de datos».*