BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-61
Fecha de publicación: 01/11/2024
Tema: Explotación activa de vulnerabilidad crítica en Microsoft SharePoint Server
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Microsoft SharePoint Server

- SharePoint Server Subscription Edition
- SharePoint Server 2019
- SharePoint Enterprise Server 2016

Descripción

Recientemente empezó a explotarse activamente la vulnerabilidad identificada como **CVE-2024-38094** en **Microsoft SharePoint Server,** publicada por Microsoft en julio pasado.

Esta vulnerabilidad está siendo un objetivo para grupos de amenazas persistentes avanzadas (**APT**) y **operadores de ransomware**, quienes utilizan esta debilidad para comprometer redes corporativas con fines de espionaje, robo de información confidencial y preparación para ataques de ransomware. Los atacantes están interesados en acceder a servidores de SharePoint debido a la gran cantidad de datos sensibles que almacenan y a las integraciones que tienen con otros sistemas, lo que facilita un alcance amplio a la red comprometida. La vulnerabilidad se debe a una falla de deserialización de datos no confiables que permite la ejecución remota de código. Un atacante autenticado con permisos de propietario del sitio puede inyectar y ejecutar código malicioso en el servidor SharePoint, comprometiendo la confidencialidad, integridad y disponibilidad del sistema.

La explotación de esta vulnerabilidad, sin embargo, requiere que el atacante previamente haya adquirido privilegios elevados dentro del sitio de SharePoint, específicamente permisos de propietario.

Solución

Se recomienda aplicar las actualizaciones de seguridad proporcionadas por Microsoft que abordan esta vulnerabilidad, las cuales se pueden encontrar en los siguientes links dependiendo de la versión de Sharepoint con la que se cuente:

SharePoint Server Subscription Edition:

- Actualización de seguridad KB5002606 (9 de julio de 2024):
  - Descripción de la actualización
  - Descarga directa

SharePoint Server 2019:

- Actualización de seguridad KB5002617 (9 de julio de 2024):
  - Descripción de la actualización
  - Descarga directa

SharePoint Enterprise Server 2016:

- Actualización de seguridad KB5002618 (9 de julio de 2024):
  - Descripción de la actualización
  - Descarga directa

Además, es aconsejable revisar y restringir los permisos de usuario en los sitios de SharePoint para minimizar el riesgo de explotación. Mantener los sistemas actualizados y aplicar las mejores prácticas de seguridad es esencial para proteger los entornos de SharePoint contra amenazas potenciales.

Cabe mencionar que los usuarios de **SharePoint Online**, la versión en la nube, **no están afectados** por esta vulnerabilidad. Microsoft aplica actualizaciones y parches de seguridad de manera proactiva en sus servicios en la nube, garantizando la protección contra este tipo de amenazas.

Información adicional:

- https://www.securityweek.com/cisa-warns-recent-microsoft-sharepoint-rce-flaw-exploited-in-attacks/
- https://blog.tecnetone.com/cisa-advierte-sobre-vulnerabilidad-cve-2024-38094-en-sharepoint
- https://www.ccn-cert.cni.es/es/seguridad-al-dia/avisos-ccn-cert/12978-ccn-cert-av-11-24-actualizaciones-de-seguridad-de-microsoft.html

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com