Boletín de alerta

Boletín Nro.:
Fecha de publicación: 20/01/2025
Tema: Alerta 2025-07 Vulnerabilidad crítica en Microsoft Configuration Manager
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Microsoft Configuration Manager

Descripción

Se ha identificado una vulnerabilidad crítica, CVE-2024-43468, en Microsoft Configuration Manager (ConfigMgr), un componente ampliamente utilizado para la gestión de sistemas en entornos empresariales. Esta vulnerabilidad representa un riesgo severo para las organizaciones que dependen de este software.

Con un puntaje CVSS de 9.8, la vulnerabilidad permite a atacantes no autenticados ejecutar código remoto en los sistemas afectados, lo que puede derivar en un compromiso completo de los entornos objetivo.

Microsoft Configuration Manager, parte de la familia de productos Microsoft Intune, facilita funciones como distribución y actualización de software, inventario, gestión de configuraciones y control remoto. Sin embargo, **CVE-2024-43468** surge de dos fallas de inyección SQL no autenticadas en el servicio **MP_Location** de ConfigMgr, causadas por una validación insuficiente al procesar mensajes de cliente.

Los atacantes pueden explotar estas fallas para realizar consultas SQL arbitrarias en la base de datos de ConfigMgr con privilegios de administrador de sistemas. Esto les permite activar el procedimiento **xp_cmdshell**, ejecutando comandos de sistema de manera remota. En caso de explotación, un atacante podría implementar cargas útiles maliciosas en toda la red, afectando múltiples puntos finales simultáneamente, con consecuencias como:

a. Violaciones de datos.
b. Compromiso completo del sistema.
c. Posible despliegue de ransomware.

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 20/01/2025
Tema: Alerta 2025-07 Vulnerabilidad crítica en Microsoft Configuration Manager
Traffic Light Protocol (TLP): Amber

Investigadores de seguridad han publicado una prueba de concepto (PoC) que detalla cómo actores maliciosos podrían aprovechar esta vulnerabilidad mediante dos vectores principales:

- Inyección en MachineID: Consiste en inyectar comandos SQL maliciosos en el campo SourceID de un mensaje XML dirigido a la función vulnerable getMachineID.
- Inyección en ContentID: Explota la función getContentID utilizando un MachineID válido obtenido de la base de datos del sistema.

Solución

- Microsoft ha lanzado el parche **KB29166583** para solucionar la vulnerabilidad

Información adicional:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468
- https://cybersecuritynews.com/microsoft-configuration-manager-rce-vulnerability/
- https://learn.microsoft.com/en-us/mem/configmgr/hotfix/2403/29166583