Este documento es una traducción de la siguiente versión en inglés https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/. Esta versión traducida se proporciona únicamente para facilitar su comprensión y por motivos de conveniencia. En caso de conflicto o ambigüedad, la versión en inglés siempre prevalecerá y tendrá prioridad.

RESUMEN EJECUTIVO

Reporte preliminar posterior al incidente (PIR) de CrowdStrike: actualización de la configuración del contenido que afecta al sensor Falcon y al sistema operativo Windows (BSOD)

Panorama general

Para estar a la vanguardia de las nuevas amenazas cibernéticas en constante evolución, los productos de seguridad actualizan el contenido de forma rutinaria. Estas actualizaciones pueden incluir la recopilación de telemetría, nuevos patrones de detección de amenazas, detección de vulnerabilidades y otras mejoras cruciales. Al actualizar de forma periódica, los productos de seguridad pueden adaptarse rápidamente a las amenazas emergentes, garantizando una protección elevada para los usuarios y sus sistemas.

Qué sucedió: resumen del incidente

El 19 de julio de 2024, a las 04:09 UTC, se publicó una actualización de Rapid Response Content ("contenido de respuesta rápida") para el sensor Falcon en el host con sistema operativo Windows que ejecuta la versión de sensor 7.11 y superior. Esta actualización debía recopilar telemetría sobre nuevas técnicas de amenazas observadas por CrowdStrike, pero provocó bloqueos (BSOD) en los sistemas que estaban en línea entre las 04:09 y las 05:27 UTC. Los hosts con sistema operativo Mac y Linux no se vieron afectados. Los hosts con sistema operativo de Windows que no estaban en línea o que no se conectaron durante este período no se vieron afectados.

Por qué sucedió: causa del incidente

Los bloqueos se debieron a un defecto en el Rapid Response Content que no se detectó durante el proceso de validación. Cuando el sensor Falcon cargó el contenido, se produjo una lectura de memoria fuera de los límites, lo que provocó bloqueos de Windows (BSOD).

¿Qué está haciendo CrowdStrike para que esto no vuelva a suceder?

Mejorar los procedimientos de prueba de software

- Mejorar las pruebas de Rapid Response Content mediante el uso de tipos de pruebas, como pruebas locales por parte de desarrolladores, actualización y reversión de contenido, estrés, fuzzing, inyección de errores, estabilidad y pruebas de interfaz de contenido.
- Introducir pruebas de validación adicionales en el validador de contenido para evitar problemas similares.

Mejorar la resiliencia y la capacidad de recuperación

- Fortalecer los mecanismos de manejo de errores en el sensor Falcon a fin de garantizar que los errores de contenido problemático se gestionen correctamente.

Refinar la estrategia de implementación

- Adoptar una estrategia de implementación escalonada, comenzando con un despliegue de valor controlado en un pequeño subconjunto de sistemas antes de un despliegue por etapas adicional.
- Mejorar la supervisión del rendimiento del sensor y del sistema durante el despliegue escalonado de contenido para identificar y mitigar los problemas prontamente.
- Proporcionar al cliente un mayor control sobre la actualización de Rapid Response Content al permitir la selección granular de cuándo y dónde se despliegan estas actualizaciones.
- Proporcionar notificaciones de actualización de contenido y los horarios previstos para ello.

Validación de terceros

- Realizar varias revisiones independientes del código de seguridad de terceros.
- Realizar revisiones independientes del proceso de calidad de extremo a extremo, desde el desarrollo hasta la implementación.