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 para mayor claridad. En caso de conflicto o ambigüedad, la versión en inglés siempre prevalecerá y tendrá prioridad.

RESUMEN EJECUTIVO

Informe preliminar posterior al incidente (Post Incident Review, o PIR) de CrowdStrike: actualización de la configuración del contenido que ha afectado al Sensor Falcon y al sistema operativo Windows (BSOD o pantalla azul)

Descripción general

Para adelantarse a las ciberamenazas que van surgiendo o que están en constante evolución, los productos de seguridad ofrecen actualizaciones de contenido de forma rutinaria. Estas actualizaciones pueden incluir la recopilación de telemetría, nuevos patrones de detección de amenazas, detecciones de vulnerabilidades y otras mejoras cruciales. Con estas actualizaciones periódicas, los productos de seguridad pueden adaptarse rápidamente a las amenazas emergentes, lo que garantiza una protección sólida a los usuarios y sus sistemas.

Qué ha ocurrido: resumen del incidente

El 19 de julio de 2024, a las 04:09 UTC, se publicó una actualización del Contenido para Respuesta Rápida para el sensor Falcon destinada a los hosts con sistema operativo Windows con la versión 7.11 o superior del sensor. El propósito de esta actualización era recopilar telemetría sobre nuevas técnicas de amenazas observadas por CrowdStrike, pero acabó provocando bloqueos (BSOD o pantalla azul) 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 Windows que no estaban en línea o no se conectaron durante ese intervalo de tiempo no se vieron afectados.

Por qué ha ocurrido: causa del incidente

Los bloqueos se debieron a un defecto en el Contenido para Respuesta Rápida, que no se detectó durante las pruebas de validación. Cuando el sensor Falcon cargó el contenido, provocó una lectura de memoria fuera de límites, lo que desencadenó los bloqueos de Windows (BSOD o pantalla azul).

¿Qué va a hacer CrowdStrike para evitar que esto vuelva a suceder?

Mejorar los procedimientos de prueba del software

- Mejorar las pruebas del Contenido para Respuesta Rápida mediante el uso de pruebas locales por parte de desarrolladores, las de actualización y reversión de contenido, de estrés, fuzzing (exploración de vulnerabilidades mediante datos aleatorios), de inserción de errores, de estabilidad y de la interfaz de contenido.
- Introducir pruebas de validación adicionales en el Validador de Contenido para prevenir sucesos similares.

Mejorar la resiliencia y la capacidad de recuperación

- Fortalecer los mecanismos de control de errores en el sensor Falcon para garantizar una correcta gestión de los errores debidos a contenidos problemáticos.

Perfeccionar la estrategia de implementación

- Adoptar una estrategia de implementación escalonada, comenzando con una implementación con valores controlados (canary) en un pequeño subconjunto de sistemas antes del despliegue por etapas.
- Mejorar la supervisión del comportamiento del sensor y del sistema durante la implementación escalonada del contenido para identificar y mitigar los problemas prontamente.
- Proporcionar a los clientes un mayor control sobre la entrega de las actualizaciones de Contenido para Respuesta Rápida, permitiéndoles una selección detallada de cuándo y dónde implementar estas actualizaciones.
- Enviar notificaciones sobre las actualizaciones de contenido y los horarios previstos.

Validación por terceros

- Encargar múltiples revisiones del código de seguridad a terceras partes (empresas independientes).
- Realizar revisiones independientes de los procesos de calidad de principio a fin, desde la fase de desarrollo hasta la implementación.