Taller de Habilidades prácticas en el ciberespacio

Estudiante:

MY. Hardy Ferney García Rodríguez

MY. Nicolas Rubio

MY. Néstor Andrés Ardila Caviedes

MY. Carlos Andrés Ríos Moncayo

Docente

Dr. Jaider Ospina Navas

Escuela Superior de Guerra

"General Rafael Reyes Prieto"

Bogotá D.C, 2024

1. análisis del caso Crowd Strike

El evento CrowdStrike se centra en una falla a nivel de actualización de ChannelFiles, que es un componente crítico en el sistema operativo Windows utilizado para la comunicación entre procesos y sistemas. Esta falla tiene implicaciones importantes en la seguridad y operatividad del sistema.

1.1 Análisis Técnico

Anillo 0 (Kernel del SO): La falla no se origina en el núcleo del sistema operativo, lo cual es positivo ya que los problemas en este nivel suelen ser críticos y difíciles de mitigar.

Anillo 1 (Componentes del SO fuera del Kernel): La falla afecta componentes de este nivel, lo que sugiere que la seguridad del SO no está completamente comprometida, pero sí existen vulnerabilidades significativas.

Anillo 2 (Controladores y utilidades del SO): Los ChannelFiles, al encontrarse en este nivel, indican que la falla está relacionada con la abstracción del hardware y los controladores del sistema de archivos, impactando directamente en la interacción con los dispositivos de hardware.

Anillo 3 (Programas y aplicaciones): La comunicación y evaluación de canales nombrados en sistemas Windows, como parte de las aplicaciones y programas, están directamente involucradas en la falla.

1.2 Análisis Práctico

Efectos Focales: Las fallas y vulnerabilidades sectoriales específicas indican que ciertos segmentos del sistema operativo son más susceptibles a ser afectados por la actualización defectuosa de ChannelFiles.

Efectos Conocidos: La materialización de fallas en componentes específicos sugiere que hay áreas identificables del sistema que están particularmente vulnerables.

Efectos Latentes: La interacción entre diferentes componentes y sectores del sistema que resultan en vulnerabilidades latentes puede indicar problemas de diseño o implementación en la arquitectura del sistema operativo.

Efectos Dominó: La cadena de anomalías y eventos inciertos en todo el sistema destaca la gravedad de la falla, ya que una vulnerabilidad puede desencadenar múltiples problemas a lo largo del sistema operativo.

2. lecciones aprendidas

a. Entender el contexto de ejecución: Es crucial analizar cómo interactúan los diferentes componentes del sistema y comprender el nivel de acoplamiento entre ellos. Esto ayuda a identificar puntos críticos y predecir posibles fallas.

b. Focalizar el análisis: Confinar los efectos de una falla en un segmento específico permite abordar y mitigar vulnerabilidades de manera más efectiva, evitando que se propaguen.

c. Acciones proactivas: No esperar a que el sistema falle según lo esperado, sino buscar activamente posibles puntos de falla y tomar medidas preventivas para asegurar la estabilidad y seguridad del sistema.

3. Acciones de remediación

Para abordar y mitigar la falla identificada en el evento CrowdStrike, se deben tomar varias acciones de remediación tanto a nivel técnico como organizacional:

a. Actualización de ChannelFiles

Corrección del Código: Revisar y corregir el código de los ChannelFiles para asegurar que las actualizaciones no introduzcan nuevas vulnerabilidades.

b. Pruebas Rigurosas: Implementar pruebas exhaustivas en entornos de prueba que simulen diversos escenarios de uso para asegurar que las actualizaciones son seguras y funcionales antes de su implementación en producción.

c. Aislamiento y Contención

Segmentación del Sistema: Asegurar que las diferentes partes del sistema están adecuadamente aisladas para prevenir la propagación de fallas. Utilizar técnicas de contención para limitar el alcance de cualquier vulnerabilidad detectada.

d. Monitorización Continua: Implementar sistemas de monitorización continua que puedan detectar anomalías y vulnerabilidades en tiempo real, permitiendo una respuesta rápida y eficaz.

e. Actualizaciones Regulares: Establecer un calendario regular de actualizaciones de seguridad para mantener todos los sistemas y componentes protegidos contra nuevas amenazas.

f. Fortalecimiento de la Seguridad

Revisión de Políticas de Seguridad: Revisar y actualizar las políticas de seguridad para garantizar que aborden adecuadamente las nuevas vulnerabilidades y riesgos identificados.

Capacitación del Personal: Proveer capacitación continua a los empleados sobre las mejores prácticas de seguridad y la importancia de seguir los protocolos establecidos.

g. Mejora de la Arquitectura del Sistema

Revisar la Arquitectura del Sistema: Evaluar la arquitectura actual del sistema para identificar y corregir debilidades estructurales que puedan haber contribuido a la falla.

Implementar Anillos de Protección Más Robustas: Mejorar los niveles de protección y aislamiento entre los diferentes anillos del sistema para minimizar el riesgo de que fallas en un nivel afecten a otros.

4. Explicación del slide

La falla en la actualización de ChannelFiles de Falcon CrowdStrike afecta cómo el sistema evalúa los canales nombrados en Windows, cruciales para la comunicación entre procesos. En términos técnicos, el sistema operativo tiene niveles de privilegio que incluyen Anillo 0 (Kernel, con acceso completo al hardware), Anillo 1 (componentes del SO con alto nivel de confianza), Anillo 2 (controladores del sistema de archivos y utilidades), y Anillo 3 (programas y aplicaciones de usuario). La falla impacta la comunicación normal entre

procesos, lo que puede provocar varios efectos: focales (problemas limitados a áreas específicas), conocidos (fallas en componentes individuales), latentes (problemas en interacciones entre componentes de diferentes sectores), y dominó (problemas encadenados afectando múltiples partes del sistema). Para gestionar estos riesgos, es fundamental comprender cómo los componentes interactúan, limitar el impacto a áreas específicas, y actuar rápidamente para identificar y solucionar problemas. Estas estrategias ayudan a contener fallas y prevenir que se extiendan o agraven, asegurando una respuesta efectiva y reduciendo el impacto general en el sistema.

I. Referencias

Crowder, H., & Jajodia, S. (2011). Protection Rings. En H. C. A. van Tilborg & S. Jajodia (Eds.), Encyclopedia of Cryptography and Security (2da ed., pp. 758-759). Springer. https://doi.org/10.1007/978-1-4419-5906-5_758

Kizza, J. M. (2015). Guide to Computer Network Security (3rd ed.). Springer. https://doi.org/10.1007/978-3-319-16385-0

Falcon, CrowdStrike. (2023). ChannelFiles Update Issue. Recuperado de https://www.crowdstrike.com/resources/case-study-channel-files-update/