ARNOLD MANUEL BATISTA REYES

ID:1123596

ANTHONY CRUZ

ICS202-2-ALGORITMOS MALICIOSOS

Santo Domingo, República Dominicana. 08/02/2025

Investigación sobre la Incidencia CrowdStrike y Microsoft

Investigación Inicial:

CrowdStrike implementó una actualización de su software, la cual, en lugar de optimizar la seguridad y funcionalidad del sistema, abrió la puerta a un grave error que afectó su sensor Falcon. En consecuencia, muchos dispositivos con Microsoft Windows presentaron fallos críticos, comprometiendo su estabilidad y operatividad. La alerta inicial sobre el problema fue emitida por Tesserent, tras detectarse múltiples reportes de fallos en diversas regiones a nivel mundial, esta situación expuso la importancia de realizar pruebas exhaustivas antes de lanzar actualizaciones en infraestructuras críticas para evitar interrupciones masivas en los sistemas.

.

Descripción Técnica:

La vulnerabilidad se produjo por un error en un archivo de configuración del sensor Falcon, que provocó lecturas de memoria fuera de los límites permitidos en el kernel de Windows, este fallo resultó en errores de página inválidos, causando que los sistemas afectados entraran en bucles de reinicio o modos de recuperación

Impacto en las Empresas:

La interrupción provocada por la actualización defectuosa de CrowdStrike impactó en diversos sectores, incluyendo aerolíneas, bancos y entidades gubernamentales. Empresas como Delta Airlines tuvieron retrasos y cancelaciones de vuelos debido a fallos en sus sistemas, mientras que bancos como Chase y Wells Fargo experimentaron interrupciones en sus plataformas digitales, afectando transacciones y el acceso a servicios de los clientes. La crisis tuvo repercuciones en la estabilidad financiera de CrowdStrike, sus acciones cayeron más del 10% luego del incidente, reflejando la pérdida de confianza de los inversores y exponiendo la vulnerabilidad de las empresas de ciberseguridad ante fallos en sus soluciones.

Respuesta y Mitigación:

Para solucionar los errores de BSOD y garantizar que los sistemas afectados pudieran mantenerse operativos, Tesserent sugirió seguir estos pasos:

Arrancar Windows en Modo Seguro o en el Entorno de Recuperación de Windows: Esto permite que el sistema inicie con una configuración mínima, evitando la carga de controladores que puedan estar causando fallos.

Acceder al directorio C:\Windows\System32\drivers\CrowdStrike: En esta ubicación se encuentra el archivo asociado al sensor Falcon responsable del problema.

Identificar y eliminar el archivo “C-00000291.sys”: La eliminación de este archivo defectuoso evita la ejecución del error crítico.

Reiniciar el sistema en modo normal: Luego de la eliminación del archivo, los dispositivos deben poder iniciar y operar sin presentar fallos de BSOD.

Lecciones Aprendidas:

Entendí la importancia de realizar pruebas rigurosas antes de implementar actualizaciones en infraestructuras críticas y la importancia de tener planes de contingencia para revertir posibles errores. Además, la vulnerabilidad en la dependencia de soluciones de seguridad y la importancia de diversificar las estrategias de ciberseguridad.

Conclusión:

El monitoreo y una respuesta rápida y efectiva ante vulnerabilidades son esenciales para proteger las operaciones y la confianza del público de cualquier sistema. Este incidente sirve como ejemplo de los riesgos que pueden presentarse en las actualizaciones de software y la importancia de una buena gestión de la seguridad.

FUENTES:

Aparicio, R. C. (2024, julio 19). *Una actualización de la firma de ciberseguridad informática CrowdStrike, origen del fallo de Microsoft*. Agencia EFE. https://efe.com/economia/2024-07-19/actualizacion-crowdstrike-fallo-incidencias-microsoft/

Europa Press. (2024, julio 19). *Un fallo en la plataforma CrowdStrike provoca la caída de Microsoft e incidencias a nivel global en bancos y aerolíneas*. portaltic. https://www.europapress.es/portaltic/ciberseguridad/noticia-fallo-plataforma-crowdstrike-provoca-caida-microsoft-incidencias-nivel-global-bancos-aerolineas-20240719112912.html

Domenech, S. L. (2024, julio 19). *Cómo solucionar el fallo de CrowdStrike y Microsoft tras la caída*. Sofistic. https://sofistic.com/como-solucionar-el-fallo-de-crowdstrike-y-microsoft-tras-la-caida/