Asignatura

ICS202-01-ALGORITMOS MALICIOSOS

Título

Investigación sobre la Incidencia CrowdStrike y Microsoft

Profesor

ANTHONY CRUZ MARTE

Alumno:

Pedro Ángel Encarnación Martínez, ID:1121181

Investigación

El 19 de julio de 2024, un suceso de gran envergadura se produjo debido a una actualización incorrecta del agente Falcon Sensor, una solución de seguridad creada por CrowdStrike. Esta actualización tuvo un efecto directo en los sistemas operativos Windows, causando fallos en masa, pantallas azules (BSOD) y ciclos de reinicio en millones de dispositivos a nivel global. El suceso impactó en servicios vitales como aeropuertos, hospitales, bancos y compañías de transporte, provocando una interrupción nunca antes vista en las infraestructuras tecnológicas.

El motivo principal se originó en una actualización automática de un archivo de configuración, implementado a través del sistema Falcon, que presentaba un fallo de programación crítico que se relacionaba de manera equivocada con el núcleo del sistema operativo Windows.

Descripción Técnica del Problema

Desde una perspectiva técnica, la actualización fallida impactó en el archivo del núcleo csagent.sys, que constituye un componente esencial del sensor Falcon. Este documento tiene una interacción directa con las funciones del sistema operativo de nivel básico. El fallo causó una página incorrecta en el área no paginada del sistema, produciendo el código de error ***PAGE_FAULT_IN_NONPAGED_AREA***, lo que implicó un reinicio continuo de los equipos impactados.

En consecuencia, al iniciar, el sistema operativo se bloqueaba, sin capacidad de recuperación automática. Lo alarmante del suceso es que no se originó por malware o una vulnerabilidad externa, sino por una incorrecta validación interna del software de seguridad que debía evitar estas fallas.

Impacto en CrowdStrike y Microsoft

CrowdStrike sufrió un impacto significativo en su reputación y valor bursátil. El mismo día del suceso, las acciones de la empresa sufrieron una caída superior al 11%, y en los días subsiguientes registraron una pérdida acumulativa superior al 13%. Pese a que la compañía respondió con rapidez, la confianza de los usuarios corporativos se vio afectada, particularmente en áreas delicadas como la salud y el transporte.

A pesar de que Microsoft no asumió la responsabilidad directa del error, también se vio impactado. La mayoría de los sistemas afectados eran Windows, lo que provocó opiniones adversas respecto a la seguridad de la plataforma. Algunos usuarios y compañías atribuyeron a Microsoft en un principio antes de que se descubriera la verdadera causa. Esto motivó a la compañía a trabajar de cerca con CrowdStrike para atenuar la crisis y brindar ayuda a los usuarios impactados.

Respuesta y Ajuste

La reacción de CrowdStrike comprendió una serie de publicaciones técnicas que detallaron el problema y proporcionaron instrucciones para su recuperación. No obstante, dado el carácter del error, la solución exigía la intervención manual en la mayoría de los equipos, lo que complicó una recuperación ágil en entidades con miles de dispositivos impactados.

Microsoft también publicó una declaración respaldando a sus clientes y sugeriendo métodos para iniciar los sistemas de forma segura y eliminar el archivo de problemas. Ambas empresas colaboraron con equipos de tecnología de la información a nivel mundial para recuperar servicios, aunque el procedimiento resultó complicado y lento en numerosos casos. La ausencia de una función para la reversión automática de actualizaciones resultó ser una debilidad notoria.

Aprendidas Lecciones

Este suceso subrayó la importancia de examinar y robustecer los sistemas de verificación de actualizaciones antes de su implementación en la producción. Las soluciones de seguridad, al funcionar en el nivel del núcleo, poseen un enorme potencial destructivo si no se examinan correctamente. Adicionalmente, destacó la relevancia de disponer de sistemas de despliegue progresivo (rollout gradual) y validaciones por áreas o segmentos.

La comunidad de ciberseguridad también descubrió que incluso los instrumentos creados para salvaguardar pueden transformarse en riesgos si no se administran correctamente. La claridad, la reacción adecuada y la comunicación eficaz con los usuarios son fundamentales para atenuar el perjuicio en estos contextos. Este caso se analizará por años como un ejemplo de cómo una línea de código puede bloquear servicios completos a nivel mundial.

Conclusión

El suceso de CrowdStrike y Microsoft del 19 de julio de 2024 evidencia que hasta las empresas más destacadas en ciberseguridad no están libres de fallos críticos. Este fallo subrayó cómo una actualización deficiente puede impactar negativamente en millones de aparatos, impactando la vida diaria de individuos y compañías. En el ecosistema tecnológico actual, la supervisión continua, las evaluaciones rigurosas y las políticas de actualización segura no son alternativas.

Referencias bibliográficas

CrowdStrike. (2024, agosto 6). *Falcon Content Update – Preliminary Post-Incident Report*. CrowdStrike. https://www.crowdstrike.com/en-us/blog/falcon-update-for-windows-hosts-technical-details/

CrowdStrike. (2024, julio 20). *Technical Details of the Faulty Update and Remediation Steps*. https://www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/

Microsoft. (2024, julio 20). *Helping our customers through the CrowdStrike outage*. Microsoft Official Blog. https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

Wikipedia contributors. (2024, agosto). *2024 CrowdStrike-related IT outages*. Wikipedia. https://en.wikipedia.org/wiki/2024_CrowdStrike-related_IT_outages

Akdağ, M. (2024, julio 21). *Understanding the CrowdStrike Update Error and Its Impact on Microsoft*. Medium. https://medium.com/@akdag/understanding-the-crowdstrike-update-error-and-its-impact-on-microsoft

Delucia, E. (2024, julio 22). *The Access Violation That Crashed the World: Technical Insights of the BSOD in CrowdStrike's csagent.sys*. EmanueleDelucia.net. https://www.emanueledelucia.net/the-access-violation-that-crashed-the-world-technical-insights-of-the-bsod-in-the-crowdstrikes-csagent-sys/

The Verge. (2024, julio 19). *CrowdStrike and Microsoft: All the latest news on the global IT outage*.

https://www.theverge.com/24201803/crowdstrike-microsoft-it-global-outage-airlines-banking