ALERTA

Incidente de CrowdStrike y sus Implicaciones

COLCERT AL-1907-038

TLP:CLEAR

Este incidente, que no se debe a un ciberataque, ha afectado a una amplia gama de industrias desde aerolíneas, bancos y hasta medios de comunicación, como comercio minorista.

”Un fallo técnico en la plataforma de seguridad Falcon Sensor de CrowdStrike ha desencadenado una interrupción generalizada de servicios a nivel mundial.”

El Equipo de Respuesta a Emergencias Cibernéticas de Colombia – **ColCERT** ha validado con las diferentes **entidades públicas y empresas privadas,** informando que en **Colombia la afectación fue mínima y ya se encuentran restablecidos los servicios.**

Impacto en la seguridad digital Nacional:

Impacto global: Las interrupciones se han sentido en diversos sectores y regiones, afectando las operaciones diarias de numerosas empresas.

Respuesta de CrowdStrike: La compañía ha reconocido el problema, ha asegurado a sus clientes que no se trata de un ciberataque y ha proporcionado soluciones alternativas mientras trabaja en una actualización permanente.

Sistemas afectados:

Actualización problemática: Una actualización de software en la plataforma Falcon Sensor de CrowdStrike ha causado conflictos con los sistemas operativos Microsoft Windows, principalmente provocando errores de pantalla azul y dificultades para iniciar los equipos.

En la actualidad el suceso hace referencia a un mal controlador de actualización. Así que, si se está ejecutando esa versión de CrowdStrike, podría poner el ordenador en una pantalla de arranque o en una pantalla azul. Una solución es eliminar ese controlador, pero podría haber problemas con este enfoque.

Solución compartida por Microsoft:

Solución recomendada por Microsoft - Reinicios repetidos: Permitir que las máquinas se comuniquen con los servidores de CrowdStrike para descargar una posible solución.

FUENTES:

https://www.infosecurity-magazine.com/news/crowdstrike-fault-it-outages/
https://www.bleepingcomputer.com/news/security/crowdstrike-update-crashes-windows-systems-causes-outages-worldwide/
https://www.crowdstrike.com/blog/statement-on-windows-sensor-update/

COLCERT

ALERTA

Incidente de CrowdStrike y sus Implicaciones

COLCERT AL-1907-038

TLP:CLEAR

Solución compartida por Microsoft:

•**Modo seguro con red:** Acceder al sistema y eliminar manualmente el archivo del controlador problemático.

•**Soluciones alternativas - Restauración del sistema:** Utilizar una copia de seguridad si está disponible.

•**Reparación del sistema operativo:** Un proceso más complejo para sistemas con discos cifrados.

Los problemas de compatibilidad de actualizaciones son importantes para definer qué arquitectura se tiene actualmente y con qué permisos actúan los agentes del sistema.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://www.infosecurity-magazine.com/news/crowdstrike-fault-it-outages/
https://www.bleepingcomputer.com/news/security/crowdstrike-update-crashes-windows-systems-causes-outages-worldwide/
https://www.crowdstrike.com/blog/statement-on-windows-sensor-update/

COLCERT