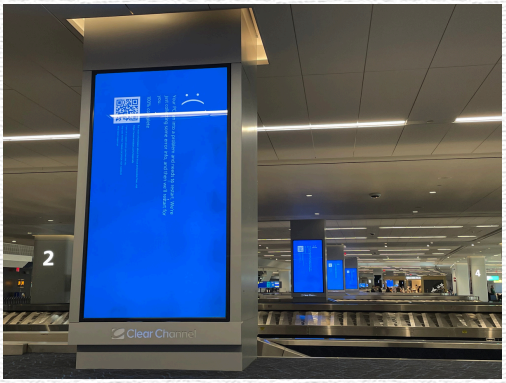
CrowdStrike

HISTORICO APAGON INFORMATICO

El 19 de julio de 2024, la empresa CrowdStrike distribuyo una actualización de configuración defectuosa para su software de sensor Falco.
Una modificación en un archivo de configuración que era responsable de la deteccion de pipes, channel file 291, provoco una lectura de memoria fuera de límites en el cliente del sensor, resultando en un invalid page fault.
Esto genero que las máquinas entraran en un bootloop o se inicien en modo recuperación.

En cuestion de horas pudieron detectar el error y se lanzo la solución pero muchas maquinas quedaron afectadas, teniendo que ser reparadas manualmente. Los apagones persistieron en muchos servicios.



Errores que llevaron a la actualizacion defectuosa

- Los archivos del canal se validaron utilizando patrones Regex con comodines y se cargaron en una matriz en lugar de utilizar un analizador para este propósito.
- La longitud de argumentos no se verificó antes del acceso. Se esperaba un input con 21 campos, pero el archivo del canal estaba en un formato de datos anterior con solo 20 campos.
- En las pruebas unitarias, solo se probó el camino feliz. No se realizaron pruebas de regresión para la compatibilidad con el formato de datos anterior.
- En las pruebas manuales, solo se probaron datos válidos.Los archivos del canal no contenían un campo de número de versión que se verificara.
- No hubo implementaciones escalonadas, pero la actualización se distribuyó a todos los clientes simultáneamente. Incluso la infraestructura crítica no recibió un trato especial.
- El software no accede al sistema en Microsoft Windows a través de una interfaz de programación de aplicaciones adecuada, sino que se ejecuta como un controlador en el anillo 0 para tener privilegios elevados en el sistema operativo. Sin embargo, un bloqueo en esta área conduce a una pantalla azul de la muerte, que detiene el sistema operativo.