devoteam
Cyber Trust

Case Study

Hackear una Smart Camera: Exposición y vulnerabilidades

Cliente

El cliente es una empresa líder en análisis de desempeño y opera en una geografía global.

Desafío

Como líder de la industria, nuestro cliente se esfuerza por introducir las últimas tecnologías en su mercado para lograr datos perspicaces de la transmisión de video en tiempo real de la cámara. El proceso utilizado para capturar video y ejecutar análisis se basa en la distribución geográfica de las cámaras que en algún momento podrán no estar conectadas a entornos de confianza y necesitarán conectarse de manera segura a la infraestructura de nuestro cliente.
Nuestro cliente nos pidió que sometiéramos su producto estrella, una cámara inteligente, a pruebas de seguridad en profundidad.

Impacto

El Proyecto Pentest ayudó al cliente a comprender los riesgos que planteaba la solución y permitió la resolución de vulnerabilidades, evitando que fueran utilizadas por atacantes reales para impactar en la organización de nuestro cliente o en los usuarios de la solución.
Confrontado con los resultados detallados en profundidad de la solución, el cliente percibió el valor de tener varias otras soluciones analizadas continuamente por el servicio KEEP-IT-SECURE-24.

Servicios Relacionados

- KEEP-IT-SECURE-24
- Pentesting
- Red Teaming

Solución

Los requisitos planteados por nuestro cliente fueron abordados por un proyecto Pentest considerando múltiples vectores de amenaza. El enfoque incluyó los siguientes escenarios:

- Se consideró el acceso físico a la cámara ya que las cámaras se colocan a menudo en áreas inseguras, y un potencial atacante puede acceder a ellas para recopilar conocimientos o comprometer el sistema;
- El acceso a la red cableada e inalámbrica a la cámara se consideró un vector válido, ya que las cámaras generalmente se colocan en redes no seguras a las que pueden acceder los posibles atacantes;
- Los endpoints de la API consumidos directamente por la cámara en nuestra infraestructura de cliente también fueron considerados.

El enfoque abarcó los siguientes pasos:

- 1er paso – investigar la solución y comprender el papel de cada bloque;
- 2er paso – realizar un ejercicio modelado de amenazas y decidir qué vectores analizar primero (red, hardware, aplicación);
- 3er planificar y ejecutar.

Algunas de las técnicas utilizadas:

- Investigar el hardware para comprender los chips y proveedores utilizados;
- Subvertir boot usando conexión en serie;
- Pruebas e conexión Wi-Fi (aplicación móvil - activación de la cámara);
- Separar el disco SSD M2 de la cámara para leer la información;
- Interceptar comunicaciones desde puertos Ethernet;
- Probar los servicios expuestos de la cámara;
- Sistema operativo de arranque (alternativo) a través de la ranura para tarjeta Micro SD;
- Instalación de la autoridad de certificación (CA) en el sistema operativo de la cámara para realizar MiTM.

El proyecto Pentest permitió el descubrimiento de múltiples vulnerabilidades importantes que fueron resueltas rápidamente por el cliente, reduciendo el riesgo para la organización del cliente y los usuarios de la solución. Los hallazgos van desde la capacidad de un atacante para acceder a las imágenes de video accediendo al almacenamiento interno de la cámara, la capacidad de comprometer la cámara e interceptar las comunicaciones y también la capacidad de comprometer el backend de análisis de la infraestructura de nuestro cliente.

Making your tech journey **more secure.**