devoteam
Cyber Trust

Case Study

Hackear uma Smart Camera: Exposições e Vulnerabilidades

Cliente

O cliente é uma empresa líder em análise de desempenho e opera numa geografia global.

Desafio

Como líder da indústria, o nosso cliente esforça-se por introduzir as mais recentes tecnologias no seu mercado, de forma a obter dados perspicazes a partir do streaming de vídeo em tempo real da câmara. O processo utilizado para capturar vídeos e executar análises baseia-se na distribuição geográfica das câmaras que, por vezes, podem não estar ligadas a ambientes de confiança e que terão de se ligar de forma segura à infraestrutura do nosso cliente. O nosso cliente pediu-nos para submetermos o seu produto estrela, uma Smart Camera, a testes de segurança profundos.

Impacto

O Pentest Project ajudou o cliente a compreender os riscos que a solução colocava e permitiu a resolução de vulnerabilidades, impedindo-as de serem utilizadas por atacantes para impactar a organização ou utilizadores da solução do nosso cliente. Confrontado com os resultados detalhados à sua solução, o cliente percebeu o valor de ter várias outras suas soluções a ser continuamente analisadas e integradas no Serviço KEEP-IT-SECURE-24.

Serviços Relacionados

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

Solução

Os requisitos apresentados pelo nosso cliente foram abordados por um projeto Pentest considerando múltiplos vetores de ameaça. A abordagem incluiu os seguintes cenários:

- O acesso físico à câmara foi considerado uma vez que as câmaras são colocadas muitas vezes em áreas inseguras, e um potencial intruso pode aceder-lhes para recolher conhecimento ou comprometer o sistema;
- O acesso à rede com fios e sem fios à câmara foi considerado como um vetor válido, uma vez que as câmaras são normalmente colocadas em redes não seguras que podem ser acedidas por potenciais atacantes;
- Os endpoints da API diretamente consumidos pela câmara na nossa infraestrutura de clientes também foram analisados.

A abordagem englobava os seguintes passos:

- 1º passo – pesquisar a solução e compreender o papel de cada bloco;
- 2º passo – faça um exercício de modelação de ameaças e decida quais os vetores a analisar primeiro (rede, hardware, aplicação);
- 3º planeamento e execução.

Algumas das técnicas utilizadas:

- Pesquisar o hardware para entender os chips e fornecedores usados;
- Subverter o boot utilizando a ligação em série;
- Testes e conexão wi-fi (aplicação móvel - ativação da câmara);
- Retirar o disco SSD M2 da câmara para ler a informação;
- Intercetar comunicações a partir das portas Ethernet;
- Testar serviços expostos da câmara;
- Sistema operativo boot (alternativa) através da ranhura do Micro SD-Card;
- Instalação da Autoridade de Certificados (CA) no sistema operativo da câmara para executar o MiTM.

O projeto Pentest permitiu a descoberta de múltiplas vulnerabilidades importantes que foram prontamente resolvidas pelo cliente, reduzindo o risco para a organização e utilizadores da solução. As descobertas vão desde a capacidade de um intruso aceder a imagens de vídeo, acedendo ao armazenamento interno da câmara, à capacidade de comprometer a câmara e intercetar comunicações e também a capacidade de comprometer o backend de análise da infraestrutura do nosso cliente.

Making your tech journey **more secure.**

Para mais informações visite
www.integrity.pt