INTEGRITY
Part of Devoteam

CASE STUDY

Hacking a Smart Camera: Exposures & Vulnerabilities

TYPE OF CLIENT

The Client is a leading performance analysis company and operates in a global geography.

CHALLENGE

As an industry leader our client strives to introduce the latest technologies in its industry in order to achieve insightful data from camera real time video streaming. The process used to capture video and execute analysis relies on the geographical distribution of cameras that sometimes might not be connected to trusted environments and will need to connect in a secure way to our client infrastructure.

Our client asked us to subject their star product, a Smart Camera, to in-depth security testing.

IMPACT

The Pentest Project helped the client to understand the risks that the solution posed and enabled the resolution of vulnerabilities, preventing them from being used by real attackers to impact our client's organisation or solution users.

Confronted with the detailed in-depth results from the camera solution Pentest, the client perceived the value of having several other solutions being continuously looked and engaged with the KEEP-IT-SECURE-24 Service.

RELATED SERVICES

- KEEP-IT-SECURE-24
- Pentesting
- RedTeaming

SOLUTION

The requirements posed by our client were addressed by a Pentest project considering multiple threat vectors. The approach included the following scenarios:

- Physical access to the camera was considered since the cameras are placed often in unsecure areas and a potential attacker can access them to gather knowledge or compromise the system;
- Wired and Wireless network access to the camera was considered a valid vector since the cameras are usually placed in unsecured networks that can be accessed by potential attackers;
- The API endpoints directly consumed by the camera on our client infrastructure were also targeted.

The approach encompassed the following steps:

- 1st step – research the solution and understand the role of each block;
- 2nd step – do a threat modelling exercise and decide which vectors to analyse first (network, hardware, application);
- 3rd plan and execute.

Some of the techniques used:

- Research the hardware to understand the chips and suppliers used;
- Subvert boot using serial connection;
- Tests and Wi-Fi enrolment (mobile app - camera activation);
- Detach the SSD M2 disk from the camera to read the information;
- Intercept communications from Ethernet ports;
- Test camera exposed services;
- Boot operating system (alternative) through the Micro SD-Card slot;
- Certificate Authority (CA) installation on the camera operating system to perform MiTM.

The Pentest project enabled the discovery of multiple important vulnerabilities that were promptly solved by the client, reducing the risk to the client's organisation and solution users. Findings range from the ability for an attacker to access to video footage by accessing internal storage of the camera, the ability to compromise the camera and intercept communications and also the ability to compromise the analysis backend of our client's infrastructure.

For more information, please visit:

- www.integrity.pt