ioXt 2020 Residential Camera Profile

Version 1.0

Document C-20-12-15-V1.0
Date 4/9/21
Document Status: Release

1. Notice of Use and Disclosure

Elements of ioXt Alliance documentation, specifications, and test plans may be subject to third party property rights, including without limitation copyrights and patents. The ioXt Alliance is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third-party intellectual property rights.

This document and information contained herein are provided on a “AS IS” basis.

THE IOXT ALLIANCE DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OF THIRD-PARTIES, OR ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR USE, TITLE, NON INFRINGEMENT, OR GUARANTEE OF PRODUCT SECURITY. IN NO EVENT WILL THE IOXT ALLIANCE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, IN CONTRACT OR IN TORT, IN CONNECTION WITH THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN.

The above notice must be included in all copies of this document.

2. Document Version Information

Version	Date	Author	Description
0.01	7/27/20	Brad Ree (ioXt)	1. Initial Draft
0.02	8/12/20	Bridgette Roberts (ioXt)	1. Comment compilation and formatting.
0.03	12/15/20	Brad Ree (ioXt)	1. Reformat to Google Doc. 2. Device scope completed 3. Threat model completed.
0.9	3/24/20	Brad Ree (ioXt)	1. Final document for board approval
1.0	4/9/21	Brad Ree (ioXt)	1. Release 1.0

1. Participants

Amit Agrawal	Amazon
Jorge Coronel	Google
Brooke Davis	Google
Shubha Gopalakrishna	Bureau Veritas
Dominick Gregory	Buzr
Gabriel Groen	ioXt
Asad Hawk	Comcast (VICE-CHAIR)
Jameson Hyde	NCC Group
Dave Kleidermacher	Google
Rutwij Kulkarni	Acumen Security
Eugene Liderman	Google
Lloyd Linder	Mobilitie
Tomislav Nad	SGS
Rebecca Onaitis	ioXt
Parthiv Parikh	SGS
Jae Park	Buzr
Suresh Pattar	iClimbSystems
Mariela Pavlova	Infineon Technologies
Brad Ree	ioXt Alliance
Bridgette Roberts	ioXt Alliance
Aron Rosenberg	Logitech (CHAIR)
Joel Scambray	NCC Group
Pawel Somietanka	Silvair, Inc.
Jordi Ventayol	Applus Laboratories
Catalin Visinescu	NCC Group

Antonio Vizcaino	Dekra
Jorge Wallace	Dekra
Simon Watson	NCC Group
Rob Wood	NCC Group

2. Introduction

2.1. Purpose

The Residential Camera profile provides a base level of security for all IP residential cameras, along with higher security levels for more advanced cameras. This profile is targeted for residential cameras, but may be used for light commercial or other deployments. The profile is focused on cybersecurity threats, with a primary focus on preventing large scale remote attacks. The profile may include some physical security protections, but does not specifically address physical or tamper style attacks for monitored security applications. However, the profile may be used in conjunction with physical security standards. The profile may also be used in conjunction with other ioXt profiles for combination devices.

Though the profile may be used for battery powered constrained cameras, the primary focus is to provide a set of baseline security requirements for powered IP cameras. Future extensions to address specific application needs may be applied. Further, other extensions such as a privacy or regional regulatory extension may also be applied.

2.2. Acronyms and Abbreviations

Acronym	Definition
OTA	Over the Air
2FA	Two-factor authentication (2FA) is an extra layer of security that uses an additional factor to validate a user's identity. A factor can be: ● Something you know - as password, answer to a "secret question" or PIN ● Something you have - a mobile phone or hardware token (e.g. Yubikey) ● Something you are - fingerprint, iris scan, face scan
PII	Personal Identifiable Information

2.3. Definitions

Term	Definition
Initialization Mode	The initialization mode is the initial state in which the product exists when first being configured by the Administrator for use in an account. Typical operations expected during this mode is network configuration, account/user configuration, cloud and device configuration, and initial firmware updates.
Management Mode	The management mode is the state in which an Administrator performs non-operational activities, such as device configuration, network configuration, account/user configuration, and firmware updates. The primary difference between the Management Mode and the Initialization Mode is Management Mode is entered from the Operating Mode of the device.
Operating Mode	The operating mode is the state in which the device is performing the primary tasks in which the device was designed to operate. The operating mode is the typical mode in which a user interacts with a device.
External storage	External storage is any storage which is accessible to the user through physical means intentionally provided by the manufacturer. Typical examples would be a SD card located inside a user accessible cavity with a sliding cover.
Known security vulnerabilities	Known security vulnerabilities are any verified vulnerability in which a researcher has submitted to the developer, vulnerabilities received from the developer of SDKs or other libraries included in the application, or vulnerabilities published in the NIST NVD for any previous versions of the developer's application.
Remote attack	Remote attacks are defined as any attack in which the attacker is not located on the local network of the device. Typically, these attacks are launched from the Internet towards the user or the server. Man in the Middle attacks are NOT remote attacks.
Proximity attack	Proximity attacks are any attack in which the attacker is within radio range of the device, or is located on the same local network as the user. The attacker may not be physically located on the local network, but may have remote control of another device on the local network.
Standard cryptography	Public cryptographic algorithms and protocols that are recommended by industry groups or standard organizations and that are considered best-practice.

Firmware	System software that ships with the device and that is provisioned during manufacturing,
Vulnerability Disclosure Program	A vulnerability disclosure program offers a channel for researchers to report security issues and vulnerabilities. A VDP may offer rewards to researchers, but is not required. A VDP must inform the researcher that the report was received, provide time estimates for a response, and then inform the research of any fixes applied to address the issue. ioXt recommends manufacturers follow ISO 29147.
Entity: User	A User has access rights to operate the product, but may be prohibited from configuration or maintenance modes. Typically, a user may not create other user accounts.
Entity: Administrator	An Administrator has access rights to install, configure, or maintain the product. An administrator may also create user accounts.
Entity: Account	The account is a collection of users and administrators which may access/control the product. Different users may have different access rights, but all fall under the control of a common administrator(s).
Sensitive account cloud data	Sensitive account cloud data for the camera profile is any data which the user deems private and should only be accessible to the users inside the account. Typical examples would include audio/video content including live and recorded content, but may not include metadata about the content. The user may grant access to the user data to monitoring services or other 3rd party services. Sensitive account cloud data for the camera profile does not include account information and device configurations which may be shared with the manufacturer or service provider.
Uniquely Encrypted	Uniquely Encrypted data refers to all the user data for an account. This user data (though it may be accessed by multiple users in the account) shall be uniquely encrypted from the user data from another account. The primary goal is to isolate user data such that accendetial access or data leaks will not expose raw sensitive user data.
Hardware Root of Trust	A hardware root of trust is the foundation on which all secure operations of a computing system depend. It contains the keys used

	for cryptographic functions and enables a secure boot process. It is inherently trusted, and therefore must be secure by design.
Debug Interface	A debug interface is any interface used by the manufacturer to configure, program, or monitor the device in the factory or repair centers. A debug interface is not used for the primary operation of the device. It should be noted that logical interfaces may be exposed on the operational interface. These logical interfaces shall be protected to the same level as a dedicated debug interface.

2.4. References

3. Profile Scope

3.1. Device expected use

- The consumer uses the device for personal video surveillance.
- The consumer uses the device for personal video communications.
- The consumer uses the device for remote video monitoring.
- The consumer uses the device as an unattended or stationary device containing video, image, or audio capture capabilities where the media stream is intended to be consumed outside of the device.
- The consumer expects that recordings stored locally or in the cloud shall be secured from remote attack and viewable only by authorized parties.
- The consumer expects that only parties explicitly authorized by the consumer should be able to view live video, hear live audio, or change settings.

3.2. Devices which are in scope

3.2.1. Device MUST include the following

- The device MUST have an interface which allows it to be connected to an IP Network.
- The device MUST include an image sensor.
- The device MUST offer a mechanism to remotely retrieve or send the media content.

3.2.2. Device MAY include the following

- The device MAY include a microphone.
- The device MAY include a speaker.

- The device MAY include motion detection capabilities.
- The device MAY include audio event detection capabilities.
- The device MAY include local, remote, or cloud storage capabilities.
- The device MAY include infrared or other illumination capabilities.
- The device MAY include Physical or Digital Pan-Tilt-Zoom (PTZ) controls.
- The device MAY include privacy controls such as a button, shutter, or setting which blocks the video and audio functionality.
- The device MAY include communications interfaces such as Wi-Fi, BLE, IEEE 802.15.4 and Ethernet.

4. Requirements

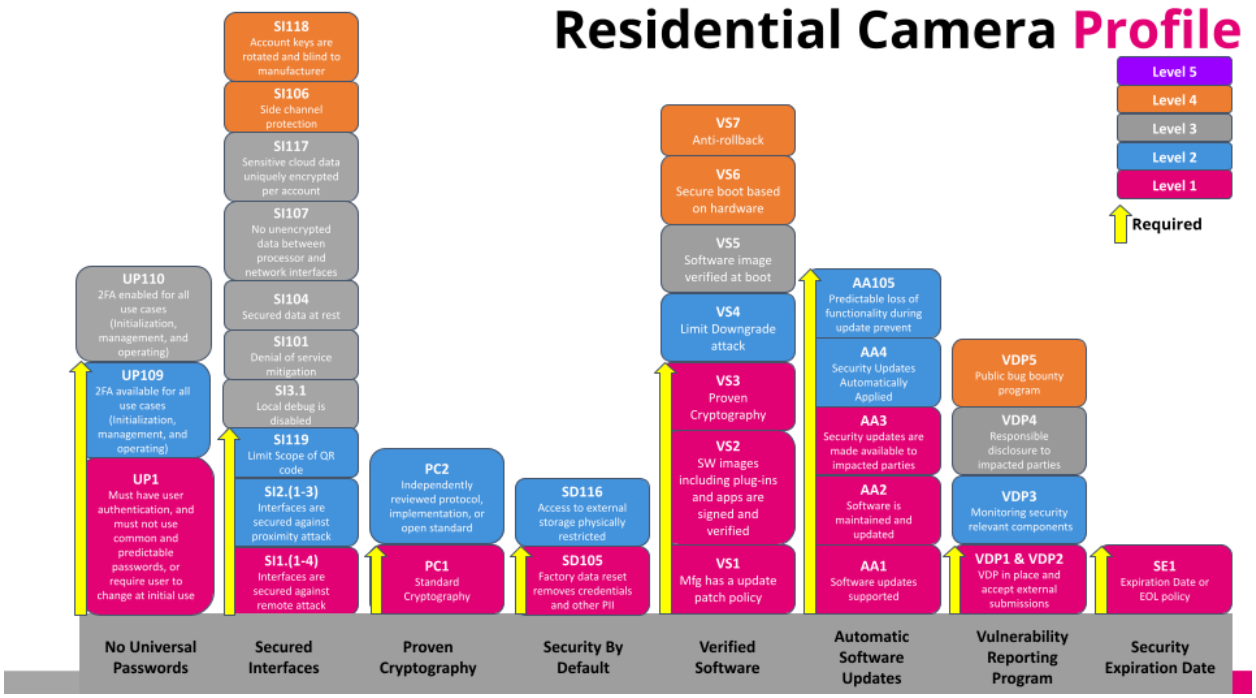
4.1. Test Case Library Version

The profile requirement document only describes the test cases needed for certification by test case ID. The actual text of the test cases are located in the ioXt Test Case Library. As the test case library is a shared document used by all profiles, there may be newer versions of the library than was approved when this profile was created.

The Residential Camera profile version 1.0 shall only use ioXt Test Case Library version 5.0.

4.2.

4.3. Profile Summary



4.4. Proven Cryptography

4.4.1. Requirements

ID	Test Case
PC1	Standard cryptography
PC2	Independently reviewed protocol, implementation, or open standard

4.4.2. Security Levels

Security Level	Test Cases	Required For Certification
1	PC1	Yes
2	PC2	

4.5. No Universal Password

4.5.1. Requirements

ID	Test Case
UP1	User credentials shall not be common or predictable, or the credentials must be required to change at initial use.
UP109	2FA is available for all use cases (initialization, management, operating)
UP110	2FA must be enabled in all use cases (initialization, management, operating)

4.5.2. Security Levels

Security Level	Test Cases	Required for Certification
1	UP1	Yes
2	UP109	Yes
3	UP110	

4.6. Verified Software

4.6.1. Requirements

ID	Test Case
VS1	Manufacturer has an update patch policy
VS2	Software images including plug-ins and apps are signed and verified
VS3	Proven Cryptography
VS4	Anti-rollback
VS5	Software images verified at boot time
VS6	Secure boot based on hardware root of trust
VS7	Anti-rollback

4.6.2. Security Levels

Security Level	Test Cases	Required for Certification
1	VS1 VS2 VS3	Yes
2	VS4	
3	VS5	
3	VS6 VS7	

4.7. Security by Default

4.7.1. Requirements

ID	Test Case
SD105	Factory data reset removes credentials and other PII
SD116	Access to external storage is physically restricted

4.7.2. Security Levels

Security Level	Test Cases	Required for Certification
2	SD105	Yes
3	SD116	

4.8. Secured Interfaces

4.8.1. Requirements

ID	Test Case
SI1.1	Remote Attack: All certifiable protocols used on the interfaces contained in the device shall be Certified
SI1.2	Remote Attack: Unused Services are disabled

SI1.3	Remote Attack: Authentication
SI1.4	Remote Attack: Secured Communications
SI2.1	Proximity Attack: Unused Services are disabled
SI2.2	Proximity Attack: Authentication
SI2.3	Proximity Attack: Secured Communications
SI119	Limit Scope of QR Codes
SI3.1	Local Attack: Debug ports are disabled or protected by authentication
SI101	Proximity Attack: Denial of Service Mitigation
SI104	Securing Data at Rest
SI107	Local Attack: No unencrypted data between processor and network interfaces
SI117	Sensitive cloud data is uniquely encrypted per account
SI106	Local Attack: Side Channel Protection
SI118	Account keys for sensitive cloud data encryption are rotated and blind to manufacturer

4.8.2. Security Levels

Security Level	Test Cases	Required for Certification
1	SI1.1 SI1.2 SI1.3 SI1.4	Yes
2	SI2.1 SI2.2 SI2.3 SI119	Yes
3	SI3.1 SI101 SI104 SI107 SI117	
4	SI106	

	SI118	

4.9. Automatically Applied Updates

4.9.1. Requirements

ID	Test Case
AA1	Software updates supported
AA2	Software is Maintained and Updated
AA3	Software updates are made available to impacted parties
AA4	Security updates applied automatically, when product usage allows.
AA105	Automatic Firmware Updates must occur at a non-predictable, random time

4.9.2. Security Levels

Security Level	Test Cases	Required for Certification
1	AA1 AA2 AA3	Yes
2	AA4 AA105	Yes

4.10. Vulnerability Reporting Program

4.10.1. Requirements

ID	Test Case
VDP1	Vulnerability Disclosure Program (VDP) in place
VDP2	Accept external submissions
VDP3	Monitoring security relevant components.
VDP4	Responsible disclosure of defects to impacted parties that must take action.

VDP5	Public Researcher Rewards program

4.10.2. Security Levels

Security Level	Test Cases	Required for Certification
1	VDP1 VDP2	Yes
2	VDP3	
3	VDP4	
4	VDP5	

4.11. Security Expiration Date

4.11.1. Requirements

ID	Test Case
SE1.1	End of life notification policy is published
SE1.2	Expiration Date is published

4.11.2. Security Levels

Security Level	Test Cases	Required for Certification
1	SE1.1 or SE1.2	Yes

5. Threat Model

This profile incorporates all the threats identified by the "Common WiFi Device" document version 1.0. Any changes below supersede the Severities identified in the common doc.

5.1. Threat Evaluation

5.1.1. Likelihood (Difficulty x Access)

Difficulty ↓ Access →	Physical Access	Proximity Access	Remote Access
Difficult	**Low**	**Medium**	**Medium**
Moderate	**Low**	**Medium**	**High**
Easy	**Medium**	**High**	**High**

5.1.2. Impact (Scope x Data access/control)

Scope ↓ Data Access/Control →	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	**Low**	**Medium**	**Medium**
Local Network	**Low**	**Medium**	**High**
Complete Fleet	**Medium**	**High**	**High**

5.1.3. Severity (Likelihood x Impact)

Likelihood↓Impact→	Low	Medium	High
Low	**Low**	**Medium**	**Medium**
Medium	**Low**	**Medium**	**High**
High	**Medium**	**High**	**High**

5.2. Provisioning

5.2.1. QR codes used for provisioning via BLE or SoftAP visible on external product

Threat Description	The QR code containing the BLE Configuration or SoftAP SSID and passphrase are leaked from the factory
Threat Agent	Product development, factory or programming location employee.
Resulting Impact	Pairing information is leaked.

5.2.1.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium			
Easy	**X**		

5.2.1.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	**X**		
Local Network			
Complete Fleet			

5.2.1.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium	**X**		
High			

5.2.1.4. Countermeasure

Test Case	None Required
Comments/Guidance	Pairing Codes can't be visible once installed or placed in service

5.3. Normal Operation - Network-based Attacks

5.3.1. NTP Attack

Threat Description	Override or force a change in the NTP servers a device uses, which can change the wall clock time reference for that device and its associated recordings.
Threat Agent	Remote attacker who gained access to the network. Local attacker who has possession of the device.
Resulting Impact	1. Video timestamps could be altered 2. Time based Actions can be bypassed (scheduled recordings, alarms, etc) 3. Expired certificates could be ignored

5.3.1.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			**X**
Moderate			
Easy			

5.3.1.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			
Local Network	**X**		
Complete Fleet			

5.3.1.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium	**X**		
High			

5.3.1.4. Countermeasure

Test Case	None Required
Comments/Guidance	Implement NTP NTS on your client device to authenticate the NTP source

5.4. Normal Operation- Physical Attacks

5.4.1. SD Card Stealing

Threat Description	User removable SD Card Stealing
Threat Agent	Local attacker
Resulting Impact	1. Video clips stolen (Private video footage)

5.4.1.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Moderate			
Easy	**X**		

5.4.1.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device		**X**	
Local Network			
Complete Fleet			

5.4.1.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium		**X**	
High			

5.4.1.4. Countermeasure

Test Case	SD116

Comments/Guidance	Physical access to the SD card should be made as difficult as possible or placed behind an additional physical control such as a screw.

5.4.2. Outdoor Physical threats around QR Code Stealing

Threat Description	Outdoor physical threats around QR code stealing.
Threat Agent	
Resulting Impact	1. Attacker steals the contents of the QR code (or equivalent).

5.4.2.1. Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Moderate			
Easy	**X**		

5.4.2.2. Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device	**X**		
Local Network			
Complete Fleet			

5.4.2.3. Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium	**X**		
High			

5.4.2.4. Countermeasure

Test Case	SI119
Comments/Guidance	The value encoded in the QR code must only allow for bootstrapping an initial secure channel (aka PAKE) and MUST NOT be a static password or other long term direct secret. There should be an additional information note about recommending that external cameras should have a removable QR code or recommendations that the consumer remove the code.

5.4.3. Laser/Blinding attack on the physical sensor.

Threat Description	Laser/Blinding attack on the physical sensor.

Threat Agent	An attacker within visual range of the device.
Resulting Impact	Attacker temporarily disables the camera to walk past “unseen”. Attacker causes false (nuisance) alarms

5.4.3.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	**X**		
Moderate			
Easy			

5.4.3.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	**X**		
Local Network			
Complete Fleet			

5.4.3.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low	**X**		
Medium			
High			

5.4.3.4. Countermeasure

Test Case	None Required
Comments	The device itself should generate a notification to its Controller that its sensor has malfunctioned or that the data being generated might no longer be valid.

5.4.4. PIR Ambient Temperature Attacks

Threat Description	PIR Ambient Temperature Attacks
Threat Agent	
Resulting Impact	Attacker disables the PIR motion sensor and thus avoids detection or raises the ambient temperature of the environment to match the body temperature of the attacker.

5.4.4.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult	**X**		
Moderate			
Easy			

5.4.4.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	**X**		
Local Network			
Complete Fleet			

5.4.4.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low	**X**		
Medium			
High			

5.4.4.4. Countermeasure

Test Case	None Required
Comments/Guidance	If possible a PIR sensor should report the detected ambient temperature to the Controller which may be able to take action if that temp changes unexpectedly.

5.4.5. Adjacent Sensor Attacks

Threat Description	Adjacent sensor attacks. Disabling a secondary sensor like the Motion Sensor.
Threat Agent	
Resulting Impact	Attacker is able to avoid detection and thus being captured on video

5.4.5.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Moderate	**X**		
Easy			

5.4.5.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device	**X**		
Local Network			
Complete Fleet			

5.4.5.3. Severity

Likelihood↓Impact→	Low	Medium	High

Low	**X**		
Medium			
High			

5.4.5.4. Countermeasure

Test Case	None Required
Comments/Guidance	

5.5. Normal Operation - Network-based Attacks

5.5.1. Man in the middle attack during video capture to cloud

Threat Description	Attacker intercepts traffic between device and cloud while video is being captured.
Threat Agent	Attacker in network path between device and cloud.
Resulting Impact	Potentially the attacker intercepting the video and streams.

5.5.1.1. Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

5.5.1.2. Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network			**X**
Complete Fleet			

5.5.1.3. Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			**X**
High			

5.5.2. Countermeasure

Test Case	SI1.1, SI1.2, SI1.3, SI1.4, SI2.1, SI2.2, SI2.3, PC1
Comments/Guidance	

5.5.3. Man in the middle attack during camera control from cloud to device

Threat Description	Attacker intercepts traffic between device and cloud over the local network while remote commands are being sent. This can include recording commands, audio talk-back, or PTZ.
Threat Agent	Attacker in network path between device and cloud.
Resulting Impact	Attacker can deny service to the device, preventing it from performing the requested command.

5.5.3.1. Likelihood

	Physical Access	**Proximity Access**	**Remote Access**
Difficult			
Medium		**X**	
Easy			

5.5.3.2. Impact

	Low sensitivity data/DoS	**Limited sensitive data/control**	**Complete compromise**
Single Device			
Local Network			**X**
Complete Fleet			

5.5.3.3. Severity

Likelihood↓Impact→	**Low**	**Medium**	**High**
Low			
Medium			**X**
High			

5.5.3.4. Countermeasure

Test Case	SI1.1, SI1.2, SI1.3, SI1.4, SI2.1, SI2.2, SI2.3, PC1 Add higher level options which include certificates.
Comments/Guidance	

5.6. Normal Operation - Functional Attacks

5.6.1. Reboots or Automated Firmware Updates while Monitoring

Threat Description	Attacker can predict when a device will be offline and not recording to visually move past the device.
Threat Agent	
Resulting Impact	Attacker can not be seen on the recordings or the live view as the device is not currently active

5.6.1.1. Likelihood

	Physical Access	Proximity Access	Remote Access
Difficult			
Medium			
Easy		X	

5.6.1.2. Impact

	Low sensitivity data/DoS	Limited sensitive data/control	Complete compromise
Single Device			X
Local Network			
Complete Fleet			

5.6.1.3. Severity

Likelihood↓Impact→	Low	Medium	High
Low			
Medium			
High		X	

5.6.1.4. Countermeasure

Test Case	AA105
Comment	Reboots or Automatic Firmware Updates must be done at a non-predictable random time.