ACME
IP Camera A2308

Document Name:	report_99200_IP_Camera_A2308_v1.0.docx
Version:	v1.0
Project Number:	99200
Date of Delivery:	June 1th, 2026
Time of Test:	May 18th, 2026 - May 22th, 2026
Author:	Tobias Hort-Giess, Compass Security Schweiz AG
Classification:	STRICTLY CONFIDENTIAL

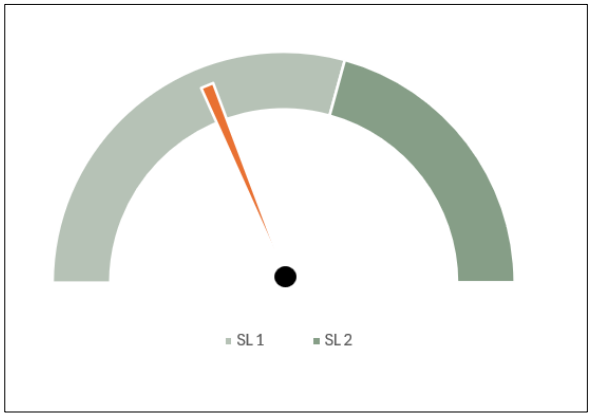
Compass Security Schweiz AG, Werkstrasse 20, CH-8640 Rapperswil
T +41 58 510 36 00, team.csch@compass-security.com, www.compass-security.com

Executive Summary

Compass Security Schweiz AG conducted an IEC 62443-4-2 component level review of the IP Camera A2308 device. This section briefly highlights the most important results and provides recommendations for future steps. Technical details are provided in subsequent chapters.

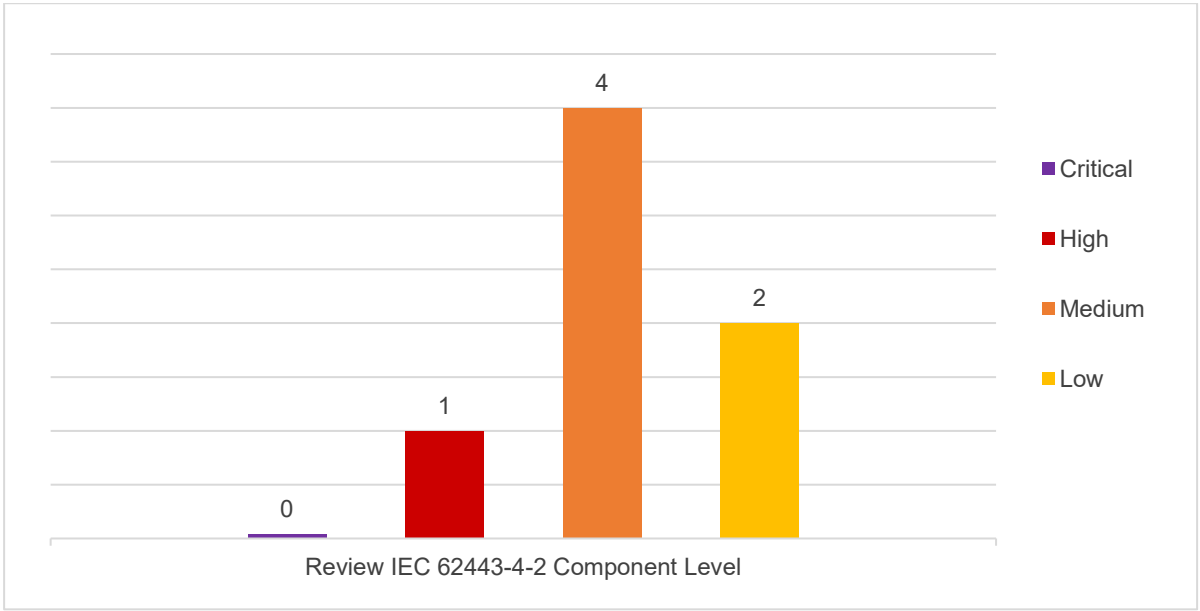
The primary objective of this assessment was to verify the device's compliance with the upcoming requirements of the Cyber Resilience Act (CRA), utilizing the IEC 62443-4-2 standard as the technical benchmark for component-level security. To conduct this evaluation, a production-ready device was delivered for rigorous investigation. The scope of the review was structured around the three distinct architectural zones identified during the initial threat modeling phase, namely the physical hardware, the network communication protocols, and the cloud integration. The assessment employed a combination of automated tools and manual testing techniques to ensure comprehensive coverage. Manual hardware testing involved evaluating the device's resistance to physical tampering, including attempts to access internal debugging interfaces, extract firmware, or perform unauthorized firmware deployment. Manual network analysis focused on the security of data in transit, specifically validating the communication link between the mobile application and the device via the cloud infrastructure.

To meet the regulatory requirements of the Cyber Resilience Act, the device is required to achieve Security Level 2 (SL2) compliance. However, this assessment concludes that the device currently does not meet any recognized Security Level. Specifically, the implementation fails to satisfy seven mandatory test cases required for Security Level 1, as well as five additional criteria necessary for Security Level 2. These gaps are primarily concentrated within the domains of authentication, authorization, and integrity.



Vulnerability Overview

The following diagram gives an overview of the identified vulnerabilities and their severity:



General Recommendations

Compass Security recommends reviewing and addressing all issues listed in the vulnerability table in chapter 2 of this report. Issues with a rating of Critical or High should be addressed immediately. All other findings can be considered as opportunities for medium- to long-term improvements.

It should be noted that the ratings assigned by Compass Security are primarily based on a technical assessment of the weakness in question. Other factors such as business impact were not necessarily considered. It is therefore recommended to carry out an internal risk assessment for each weakness.

For more information about the ratings and their definition, please refer to section 5.1 in the appendix.

Table of Contents

1 Overview

This document is intended for project teams, development personnel, and other individuals concerned with the security of the tested system. The purpose of this document is to summarize the results of the security assessment.

1.1 Document Structure

Chapter	Content
-	Executive summary
1	Document overview, scope, and procedure
2	A list of the identified weaknesses as well as suggestions for improvement
3, 4	Protocol of the performed security tests
5	Appendix

1.2 Scope and Procedures

The security assessment covered the following:

Target	Module	Effort
IP Camera A2308	M1 IEC 62443-4-2 Component Level Review	5 PD

2 Vulnerabilities and Remediation

This chapter summarizes the security issues found during the security review. A definition for each table column is given here:

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
Each issue is numbered consecutively.	Reference to the corresponding test case in the following chapters.	Explains the weakness identified during the assessment.	Explains the impact of the weakness if it were to be exploited.	Recommendation on how to address the weakness.	Compass rating of the weakness and the corresponding threat: ▪ **Critical** ▪ **High** ▪ **Medium** ▪ **Low** ▪ **Info** *See chapter 5 for a detailed rating description and color code definition.*	Comment and information provided by the customer.

2.1 Review IEC 62443-4-2 Component Level

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
1.	4.6.1 #1-3	**Device Enumeration Vulnerability** The application fails to enforce authorization checks during the registration process, allowing attackers to enumerate device IDs and register unauthorized devices.	An attacker can discover the approximate physical locations of cameras and identify potential owners, leading to privacy breaches and reconnaissance for more targeted attacks.	Implement strict authorization controls that validate user permissions and device ownership before allowing registration or any device-related queries.	**High**	
2.	4.5.1 #3,4	**Unauthenticated Local Network Video Access** Video streaming interfaces on the local network lack an authentication mechanism, allowing direct access to live feeds without credentials.	An attacker or unauthorized individual with network access to the local network can intercept sensitive visual data and monitor activities undetected.	Implement robust authentication protocols for all video streaming interfaces, regardless of network location.	**Medium**	

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
3.	4.5.4 #2 4.6.4 #2	**Unauthenticated Physical UART Shell Access** The device provides a root-level shell via physical UART pins that does not require any password or authentication to access.	An attacker with physical access to the hardware can disassemble the device and intercept the serial interface to gain full administrative control over the operating system	Implement a unique, strong password for the root shell on and disable the UART interface in production hardware.	**Medium**	
4.	4.5.5 #3	**Password Blocklist Missing** The mobile application allows users to change the password to a commonly used one or to one that has already been leaked.	An attacker can use a list of common passwords to test against multiple user accounts. The more accounts are registered the more likely common passwords are used.	Implement a comprehensive password blocklist to prevent users from choosing commonly used and known passwords.	**Medium**	
5.	4.7.9 #1,2	**Absence of Firmware Integrity** The device lacks a secure boot mechanism, allowing an attacker to physically modify the firmware and flash it onto the EEPROM chip without detection.	An attacker with physical access can overwrite the legitimate firmware with a malicious version, granting them permanent, low-level control over the device's operations.	Implement a Secure Boot process that uses cryptographic signatures to verify the integrity of the firmware before it is executed.	**Medium**	
6.	4.5.6 #2	**Unverifiable PKI for Secure Firmware Updates** The PKI used to decrypt firmware during the upgrade process is obscured, preventing verification of whether the cryptographic keys and algorithms meet required security standards.	If the obfuscated keys are recovered and found to be weak, an attacker could bypass the upgrade security to deploy malicious, unauthorized firmware to the device.	Implement a transparent and auditable PKI architecture, utilizing hardware-based security where possible, to ensure all cryptographic primitives used in the firmware update process comply with IEC 62443-3-3 requirements.	**Low**	
7.	4.7.2 #1,2	**Absence of Verifiable Security Function Monitoring and Reporting** There is no documented evidence or demonstrable process to verify that security functions operate correctly or that security anomalies are reported.	Security failures or unauthorized changes may go undetected for extended periods, leaving the system vulnerable to exploits that bypass weakened or malfunctioning security controls.	Establish and document formal procedures for the periodic verification of security functions and implement a structured reporting process for security anomalies during all lifecycle phases.	**Low**	

3 Evaluation IEC 62443-4-2 Component Level

3.1 Overview

ID	Requirement	Security Level Achieved	SL 1	SL 2
FR 1	Identification and authentication control	SL 0	9/12	2/3
FR 2	Use control	SL 0	0/1	1/4
FR 3	System integrity	SL 0	5/8	6/7
FR 4	Data confidentiality	SL 2	3/3	1/1
FR 5	Restricted data flow			
FR 6	Timely response to events			
FR 7	Resource availability			

3.2 Details

The Component Requirements written in light grey indicate that these do not apply and were therefore not selected for the device. The rationale behind it can be found in chapter in 4.4.

ID	Requirement	Security Level Achieved	SL 1	SL 2
FR 1	**Identification and Authentication Control**	**SL 0**	**9/12**	**2/3**
CR 1.1	Human user identification and authentication	SL 0	0/1	0/1
CR 1.2	Software process and device identification and authentication	SL 2	0/0	1/1
CR 1.3	Account management	SL 2	1/1	0/0
CR 1.4	Identifier management			
CR 1.5	Authenticator management	SL 0	0/1	0/0
CR 1.6	Wireless access management			
CR 1.7	Strength of password-based authentication	SL 0	3/4	0/0
CR 1.8	Public key infrastructure	SL 1	0/0	0/1
CR 1.9	Strength of public key-based authentication			
CR 1.10	Authenticator feedback	SL 2	3/3	0/0
CR 1.11	Unsuccessful login attempts	SL 2	2/2	0/0
CR 1.12	System use notification			
CR 1.13	Access via untrusted networks (see NDR 1.13)			
CR 1.14	Strength of symmetric key-based authentication			
FR 2	**Use control**	**SL 0**	**0/1**	**1/4**
CR 2.1	Authorization enforcement	SL 0	0/1	0/2
CR 2.2	Wireless use control			

ID	Requirement	Security Level Achieved	SL 1	SL 2
CR 2.3	Use control for portable and mobile devices			
CR 2.4	Mobile code			
CR 2.5	Session lock			
CR 2.6	Remote session termination	SL 0	0/0	1/1
CR 2.7	Concurrent session control			
CR 2.8	Auditable events			
CR 2.9	Audit storage capacity			
CR 2.10	Response to audit processing failures			
CR 2.11	Timestamps			
CR 2.12	Non-repudiation			
CR 2.13	Use of physical diagnostic and test interfaces	SL 1	0/0	0/1
FR 3	**System integrity**	**SL 0**	**5/8**	**6/7**
CR 3.1	Communication integrity	SL 2	1/1	1/1
CR 3.2	Protection from malicious code			
CR 3.3	Security functionality verification	SL 0	0/2	0/0
CR 3.4	Software and information integrity	SL 2	1/1	1/1
CR 3.5	Input validation	SL 2	1/1	0/0
CR 3.6	Deterministic output			
CR 3.7	Error handling	SL 2	1/1	0/0
CR 3.8	Session integrity	SL 2	0/0	3/3
CR 3.9	Protection of audit information			
CR 3.10	Support for updates	SL 2	1/1	1/1
CR 3.11	Physical tamper resistance and detection			
CR 3.12	Provisioning product supplier roots of trust			
CR 3.13	Provisioning asset owner roots of trust			
CR 3.14	Integrity of the boot process	SL 0	0/1	0/1
FR 4	**Data confidentiality**	**SL 2**	**3/3**	**1/1**
CR 4.1	Information confidentiality	SL 2	3/3	0/0
CR 4.2	Information persistence	SL 2	0/0	1/1
CR 4.3	Use of cryptography			
FR 5	**Restricted data flow**			
CR 5.1	Network segmentation			

ID	Requirement	Security Level Achieved	SL 1	SL 2
CR 5.2	Zone boundary protection (see NDR 5.2)			
CR 5.3	General-purpose person-to-person communication restrictions			
CR 5.4	Application partitioning			
FR 6	**Timely response to events**			
CR 6.1	Audit log accessibility			
CR 6.2	Continuous monitoring			
FR 7	**Resource availability**			
CR 7.1	Denial of service protection			
CR 7.2	Resource management			
CR 7.3	Control system backup			
CR 7.4	Control system recovery and reconstitution			
CR 7.5	Emergency power			
CR 7.6	Network and security configuration settings			
CR 7.7	Least functionality			
CR 7.8	Control system component inventory			

4 Review IEC 62443-4-2 Component Level

4.1 Description

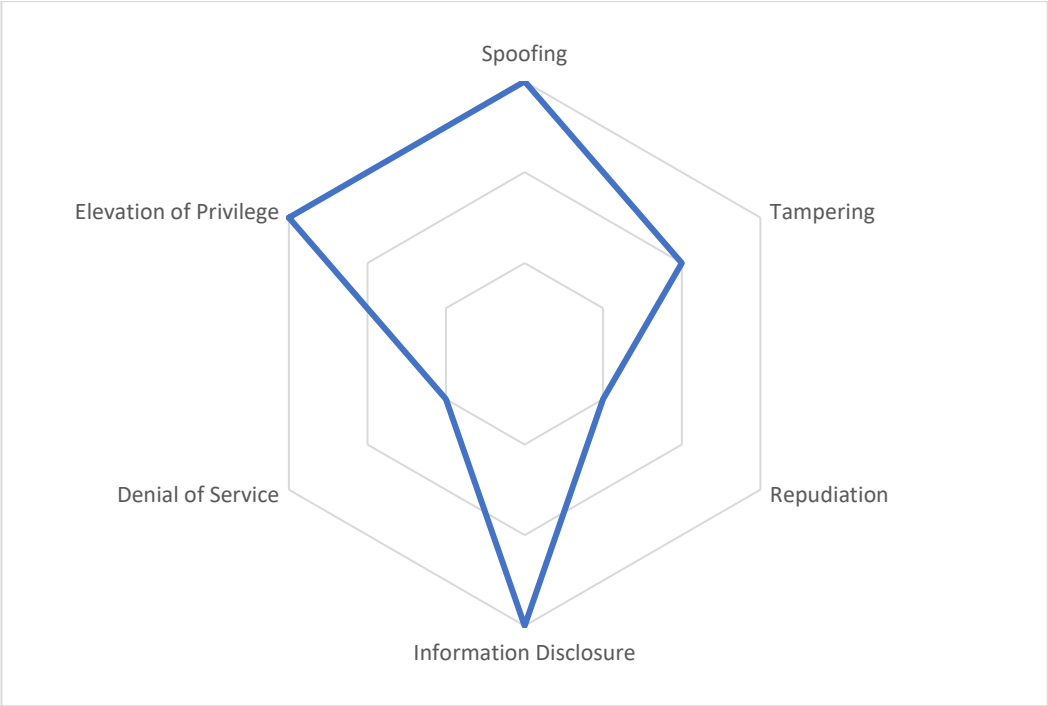
The component under test is the A2308, a networked visual sensor manufactured by Shenzhen ShunXinDa Trading Co., Ltd. The device functions as a video acquisition node that performs processing and motion detection directly on the hardware. It exposes a variety of logical interfaces, including HTTP for web management, RTSP for video streaming, and proprietary TCP/UDP protocols for cloud signaling, alongside physical interfaces such as Ethernet for network connectivity and a MicroSD slot for local storage. Architecturally, the device is not a standalone entity but is deeply integrated into a distributed ecosystem; it maintains a persistent connection to the Yoosee Cloud Infrastructure to facilitate Peer-to-Peer (P2P) connectivity, which in turn enables remote interaction via the Yoosee Mobile Application. Consequently, the device's operational lifecycle is inextricably linked to the availability and security of both the cloud backend and the mobile client interfaces.

4.2 Thread Modeling (STRIDE)

The threat model covers three zones: the device, the network (transit), and the cloud/app.

STRIDE	Threat	Vector	Rating	Rationale
Spoofing	An attacker could impersonate the Yoosee Cloud server to send malicious commands to the camera, or impersonate a legitimate user to gain access to the video feed via the mobile app.	Weaknesses in mutual authentication or identity verification between the component, the cloud, and the end-user.	**High**	Successful impersonation of the cloud or user provides the necessary entry point for all subsequent unauthorized control.
Tampering	An attacker could modify the firmware to install a backdoor or alter the device configuration (e.g., changing the destination of the video stream).	Unauthorized modification of system integrity, including firmware, configuration files, or local storage media.	**Medium**	While serious (e.g., firmware malware), it requires higher technical effort than data interception or service disruption.
Repudiation	A user or an attacker performs an action (like deleting footage or changing settings), and the device/cloud fails to log who did it.	Insufficient or non-existent audit logging within the device firmware or the Yoosee cloud management logs.	**Low**	In consumer use cases, the forensic requirement to prove "who" performed an action is significantly less critical than privacy or availability.
Information Disclosure	Unauthorized interception of the live video stream or sensitive configuration data.	Unencrypted RTSP streams over the local network or "man-in-the-middle" (MITM) attacks on the proprietary TCP/UDP cloud signaling.	**High**	The core value of the device is visual privacy; unauthorized access to the video stream is the most likely and damaging exploit.
Denial of Service	The camera becomes unavailable for monitoring, either locally or remotely, due to a flood of network traffic.	Flooding the Network interface with traffic, or an attack on the Yoosee Cloud infrastructure that breaks the P2P connection, rendering the "remote" function useless.	**Low**	Denial of Service is classified as a low-impact risk because, within this consumer price bracket, the device is intended for non-essential monitoring.
Elevation of Privilege	A user with "guest" or "viewer" permissions manages to gain "administrator" privileges to change system-wide settings.	Vulnerabilities in the HTTP web management interface (e.g., broken access control) or exploiting a flaw in the device's command-parsing logic.	**High**	Allows an unauthorized user to bypass restrictions, potentially gaining administrative control over the device and the local network.

Threat Profile



4.3 Security Level

The A2308 can be classified as an **Important Class I** product under the **Cyber Resilience Act (CRA)**. This classification is justified by the device's core functionality and underscored by the CRA itself, which explicitly lists **"smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems"** under **Annex III**.

Given the device's classification as an Important Class I product under the CRA, the security requirements must transcend basic accidental protection. Therefore, the A2308 should aim to achieve **Security Level 2 (SL 2)** according to **IEC 62443-4-2**. This level is appropriate as it provides a defense-in-depth posture against intentional, non-targeted attacks and the use of common exploit tools. Achieving SL 2 ensures that the device provides the necessary level of integrity and confidentiality required for a component explicitly recognized by the CRA as a critical element of smart home security functionality.

4.4 Rationale for Not-Selected Component Requirements

For all CRs that are not selected from the standard SLs as defined in IEC 62443-4-2, a rationale is given in the following table.

ID	Requirement	Rationale
CR 1.4	Identifier Management	Lack of important relevance for consumer device.
CR 1.6	Wireless Access Management	Not applicable
CR 1.9	Strength of public key-based authentication	Not applicable
CR 1.12	System use notification	Not applicable
CR 1.13	Access via Untrusted Networks	Not applicable
CR 1.14	Strength of symmetric key-based authentication	Not applicable
CR 2.2	Wireless Use Control	Not applicable
CR 2.3	Use Control for Portable and Mobile Devices	There are no component-level requirements
CR 2.4	Mobile Code	Not applicable
CR 2.5	Session lock	Not applicable

ID	Requirement	Rationale
CR 2.7	Concurrent Session Control	Applies for Security Level 3 and above.
CR 2.8	Auditable Events	Omitted, as threat modeling identified repudiation as a low-impact risk.
CR 2.9	Audit Storage Capacity	Omitted, as threat modeling identified repudiation as a low-impact risk.
CR 2.10	Response to Audit Processing Failures	Omitted, as threat modeling identified repudiation as a low-impact risk.
CR 2.11	Timestamps	Omitted, as threat modeling identified repudiation as a low-impact risk.
CR 2.12	Non-Repudiation	Omitted, as threat modeling identified repudiation as a low-impact risk.
CR 3.2	Protection from Malicious Code	Not applicable
CR 3.6	Deterministic output	Not applicable
CR 3.9	Protection of Audit Information	Omitted, as threat modeling identified repudiation as a low-impact risk.
CR 3.11	Physical Tamper Resistance and Detection	Not applicable
CR 3.12	Provisioning Product Supplier Roots of Trust	Not applicable
CR 3.13	Provisioning Asset Owner Roots of Trust	Not applicable
CR 4.3	Use of Cryptography	Not applicable
FR 5	Restricted data flow	Not applicable
FR 6	Timely response to events	Omitted, as threat modeling identified repudiation as a low-impact risk.
FR 7	Resource availability	Omitted, as threat modeling identified denial of service as a low-impact risk.

4.5 FR 1 – Identification and Authentication Control

4.5.1 CR 1.1 Human User Identification and Authentication

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	What interfaces does the device provide?	For example FTP, SSH, HTTP, etc.	The device exposes 5000/tcp, HTTP interface with SOAP on top for ONVIF. Also the device exposes 554/tcp, the Real Time Streaming Protocol (RTSP).	**N/A**
2.	How is authentication performed?	E.g. passwords, tokens, physical keys, etc.	For cloud: Username and password. No, MFA enforcement. No authentication is needed to access video stream directly in local network.	**N/A**

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
3.	Do all interfaces which are accessed by human users authenticate all human users?	Yes.	No, no authentication is needed when accessing video stream directly in local network.	**FAIL**
SL-C 2				
4.	Do all interfaces provide the capability to uniquely identify and authenticate all human users?	Yes.	In consequence of the above.	**FAIL**

Details #3,4

For accessing the video stream on the local network the following command can be used. There is no authentication mechanism.

```
$ ffplay rtsp://192.168.50.77:554/onvif1
```

4.5.2 CR 1.2 – Software Process and Device Identification and Authentication

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	What other components does the assessed component interact with?	E.g. other applications, embedded devices, host devices, network devices.	With the cloud/mobile app.	**N/A**
SL-C 2				
2.	Does the component provide the capability to authenticate to all other components it interacts with?	Yes.	Yes.	**PASS**

4.5.3 CR 1.3 – Account Management

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Does the component allow the management of all accounts?	Yes, either directly or via a higher-level account management system it is integrated into.	Via the app.	**PASS**

4.5.4 CR 1.5 – Authenticator Management

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	What kinds of authenticators are supported?	E.g. tokens, keys, biometrics, passwords, physical keys etc.	Password.	**N/A**
SL-C 1				
2.	Is a secure initial authenticator set in all instances?	Yes. E.g. no default passwords and appropriately long keys.	No. On the device it self it is possible to get shell access with root privileges without password. See 4.6.4 #2.	**FAIL**

4.5.5 CR 1.7 – Strength of Password-Based Authentication

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Does the component provide the capability to enforce a configurable password strength?	Yes.	Mobile app: yes.	**PASS**
2.	Does the component allow the use of set weak passwords?	No, complexity and minimum length requirements should be configured accordingly.	Mobile app: yes.	**PASS**
3.	Is it possible to set commonly known passwords?	No, a blacklist should be implemented.	Mobile app. yes.	**FAIL**
4.	Are human users able to change their password?	Depending on the component.	Mobile app: yes.	**PASS**

4.5.6 CR 1.8 – Public Key Infrastructure

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is a PKI used?	-	Yes, for firmware updates. The firmware updates are encrypted asymmetrically and need to be decrypted on the device before applying it.	**N/A**
SL-C 2				
2.	Does the component use a PKI that is in accordance with IEC 62443-3-3?	Yes.	This could not be evaluated. The private key located on the firmware in some form obfuscated, encoded or encrypted.	**FAIL**

Details #1,2

It was possible to record the update process on the device. The device downloads the latest firmware from http://dev-1251981983.cos.ap-beijing.myqcloud.com/. The firmware is encrypted though. The decryption is handled by the rsa_dec binary on the device. This indicates that RSA (asymmetric encryption) is used.

The decryption logic found in /bin/gwellupdater.sh:

```
export RSA_KEYPATH=/etc/keyrsa
echo $RSA_KEYPATH
```

```
#decryption (FILENAME usually with upg.bin.enc)
echo "Decrypting $FILENAME"
[ X"temp" != X${FILENAME:0:4} ] && RSA_DEC_O=-o
rsa_dec $RSA_DEC_O -v -f $FILENAME #1>/dev/null
if [ $? -ne 0 ]; then
  #amrplayer /res/sound/set_fail.amr
  #upg_end "rsa_dec error! Wrong platform???"

  if [ ! -f /tmp/do_not_reboot_after_update ]; then
    echo -e "$1:  We need \e[1;31mreboot\e[0m."
    reboot
  else
    echo -e "$1: Ready. (\e[35mno need reboot\e[0m)"
  fi
fi
```

The recorded update process:

```
[CUT BY COMPASS]
vKey_DrvProc [940] exit >>>
main 24248 dwExitOption = 2, EXIT_UPGRADE=2
UpgFirmWareProc UPG_FILE:/mnt/ramdisk/temp_upg.bin.enc
total used free shared buff/cache available
Mem: 27296 11436 3432 6104 12428 8552
Swap: 0 0 0
It is running /mnt/ramdisk/ipc_gwellupdater.sh(copy from /ipc/sbin/ipc_gwellupdater.sh)
now...
Error ! exit !
vNPCExit Exit by signal:15killall: shell_debug: no process killed
kill shell_debug success
killall: wpa_supplicant: no process killed
killall: wpa_supplicant: no process killed
kill wpa_supplicant success
Wifi type: 8188fu
rmmod: can't unload module 'rtl8188fu': No such file or directory
drop caches 1
/etc/keyrsa
Decrypting /mnt/ramdisk/temp_upg.bin.enc
encryption method: quick (rng)
key: 2203g2Mak330s
encryption level: 256
decrypting: /mnt/ramdisk/temp_upg.bin.enc
plaintext file: /mnt/ramdisk/temp_upg.bin
[ ].....................................................................
/mnt/ramdisk/temp_upg.bin.enc
25
drop caches 2
[CUT BY COMPASS]
```

For decryption the private key named 2203g2Mak330s in /etc/keyrsa is used. The key seems to be stored in a non-standard binary format:

```
$ cat etc/keyrsa/2203g2Mak330s.prv | head -c 256 | hexdump -C
00000000  49 41 53 52 53 41 b6 98  83 88 5f a9 1c bf 33 7b  |IASRSA...._...3{|
00000010  9d 85 ad 31 c9 05 00 00  00 00 00 00 00 00 01 00  |...1............|
00000020  00 00 b5 25 61 8c 87 31  ea f1 94 b5 09 e0 2b 70  |...%a..1......+p|
00000030  c7 09 00 00 00 00 00 00  00 00 01 00 00 00 63 08  |..............c.|
00000040  84 8d 6e 76 e7 10 3f 65  52 0d 84 28 da 0a 00 00  |..nv..?eR..(....|
00000050  00 00 00 00 00 00 01 00  00 00 cb 0c 96 e2 fb 77  |...............w|
00000060  37 47 d8 2c 2a 15 db 0b  a1 02 00 00 00 00 00 00  |7G.,*...........|
00000070  00 00 01 00 00 00 cd 2e  a7 2a b1 af 35 89 7e b0  |.........*..5.~.|
00000080  a0 d6 62 d6 50 fa b3 55  00 d6 35 8f 9c 3d d1 08  |..b.P..U..5..=..|
00000090  83 7a bf 5f e8 82 00 00  00 00 00 00 00 00 03 00  |.z._............|
000000a0  00 00 4f c3 55 25 ae c8  5f 06 70 80 83 64 72 06  |..O.U%.._.p..dr.|
000000b0  89 9b 7f 1f b1 7a 31 08  fb 93 cd 7c a8 03 ca 18  |.....z1....|....|
000000c0  aa 84 00 00 00 00 00 00  00 00 03 00 00 00 b9 c8  |................|
000000d0  c3 fa dd 48 5c fb 47 87  e1 e2 aa 9d 10 a9 a8 0a  |...H\.G.........|
000000e0  94 cc ee 96 d2 fe 8e 21  ab b7 c2 25 18 09 00 00  |.......!...%....|
000000f0  00 00 00 00 00 00 03 00  00 00 f3 8c 7a 67 bc c2  |............zg..|
```

4.5.7 CR 1.9 – Strength of Public Key-Based Authentication

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the component use public-key based authentication?	-	No.	**N/A**

4.5.8 CR 1.10 – Authenticator Feedback

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Is all feedback of authenticator information obscured?	Yes. For example displaying asterisks when a human user types a password or not providing hints as to the reason why authentication failed like "unknown user name".	Yes.	**PASS**

4.5.9 CR 1.11 – Unsuccessful Login Attempts

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Does the component enforce a limit of invalid access attempts during a reasonable timeframe?	Yes.	Yes.	**PASS**
2.	Does the component deny access for a reasonable timeframe or until unlocking by an administrator if this enforced limit is reached?	Yes.	Yes.	**PASS**

4.5.10 CR 1.12 – System Use Notification

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	When a component provides local user access, is there a system use message displayed before authenticating?	Yes. This can include remarks regarding the asset owner, that actions by the user are monitored or that the unauthorized use is prohibited.	This test case is not security-relevant. The presence or absence of a system use message prior to authentication does not materially impact the security of the system, as it is purely informational and does not enforce or enhance access control.”	**N/A**

4.5.11 CR 1.14 – Strength of Symmetric Key-Based Authentication

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is symmetric-key authentication used?	-	No.	**N/A**

4.6 FR 2 - Use Control

4.6.1 CR 2.1 – Authorization Enforcement

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Does the component provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities?	Yes.	No. The application is vulnerable to device ID enumeration and unauthorized device registration. While this flaw does not grant access to live video streams, it enables an attacker to discover approximate camera locations and identify potential owners.	**FAIL**
SL-C 2				
2.	Does the component provide an authorization mechanism for all users (humans, software, devices) based on their responsibilities according to the least privilege principle?	Yes.	In consequence of the above.	**FAIL**
3.	Does the component provide for an authorized role to define and modify the mapping of permissions to roles for all human users?	Yes, either directly or through a compensating security mechanism.	In consequence of the above.	**FAIL**

Details #1

The following HTTP request illustrates the device registration process. It demonstrates that the DeviceID is a sequential integer, making the endpoint highly susceptible to enumeration attacks.

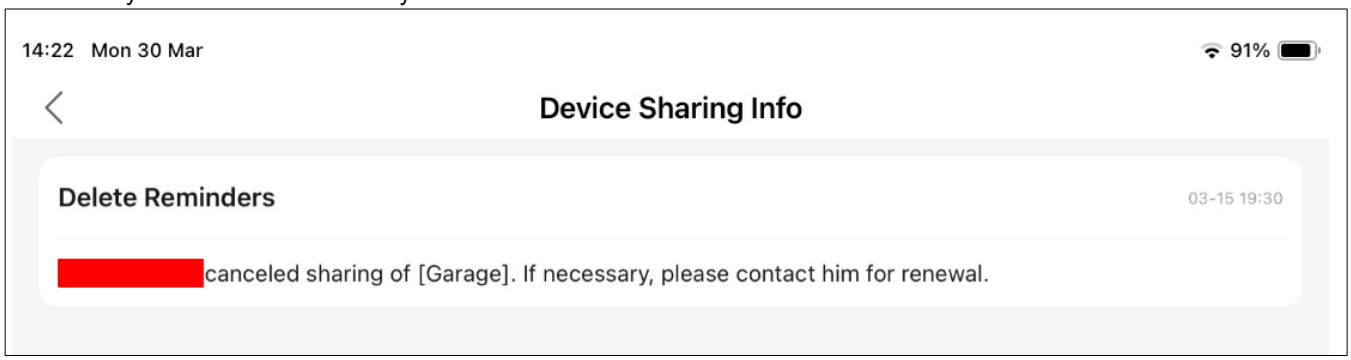
```
POST /Relationship/AddDevice.ashx HTTP/1.1
Host: api4.cloud-links.net
Accept: */*
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate, br
User-Agent: Yoosee/23 CFNetwork/3826.600.41.2.1 Darwin/24.6.0
Accept-Language: en-GB,en;q=0.9
Content-Length: 415
Connection: keep-alive

ModifyTime=1773311946&ApiVersion=1&AppToken=60ded395c2bdad3a2610ac6150550f551bb911eb6e6f7106
c40c3bb1457bb07d&AppVersion=3016231&RemarkName=Garage&PackageName=com%2Eco%2EYoosee&DeviceIn
foVersion=0&GroupID=0&SessionID=1150489714&Language=en&AppOS=2&AppID=adf33ae6eaa1439b48841fc
330ffef11&AppName=Yoosee&DeviceID=37901924&Permission=271&UserID=0139795331&SecretKey=jGr%2F
5K%2BnjjqbdaqgeEuIftLMYRac07tAc8U26%2FxvoEA%3D
```

Successful registration attempts using enumerated DeviceIDs may return the approximate geographic location of the device in the server response:

```
[
  { "deviceId": "37901981",
    "deviceName": "Garage",
    "status": "2",
    "areaSupport": 0,
    "area": "BR|27|Avare",
    "eventStatus": "2"
  },
  {
    "deviceId": "37901916",
    "deviceName": "Garage",
    "status": "2",
    "areaSupport": 0,
    "area": "CA|ON|Barrie",
```

```
    "eventStatus": "2"
  },
  {
    "deviceId": "37901904",
    "deviceName": "Garage",
    "status": "2",
    "areaSupport": 0,
    "area": "US|PA|Philadelphia",
    "eventStatus": "2"
  },
  {
    "deviceId": "37901938",
    "deviceName": "Garage",
    "status": "2",
    "areaSupport": 0,
    "area": "IT|UNKNOWN|UNKNOWN",
    "eventStatus": "2"
  },
[CUT BY COMPASS]
```


The application's registration logic appears to grant shared access. If access is revoked by the owner, the application inadvertently leaks the owner's identity.



4.6.2 CR 2.5 – Session Lock

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the component provide a human interface either locally or via a network?	-	No not in that sense. The only human interface would be the mobile phone where session locking should be configured.	**N/A**

4.6.3 CR 2.6 – Remote Session Termination

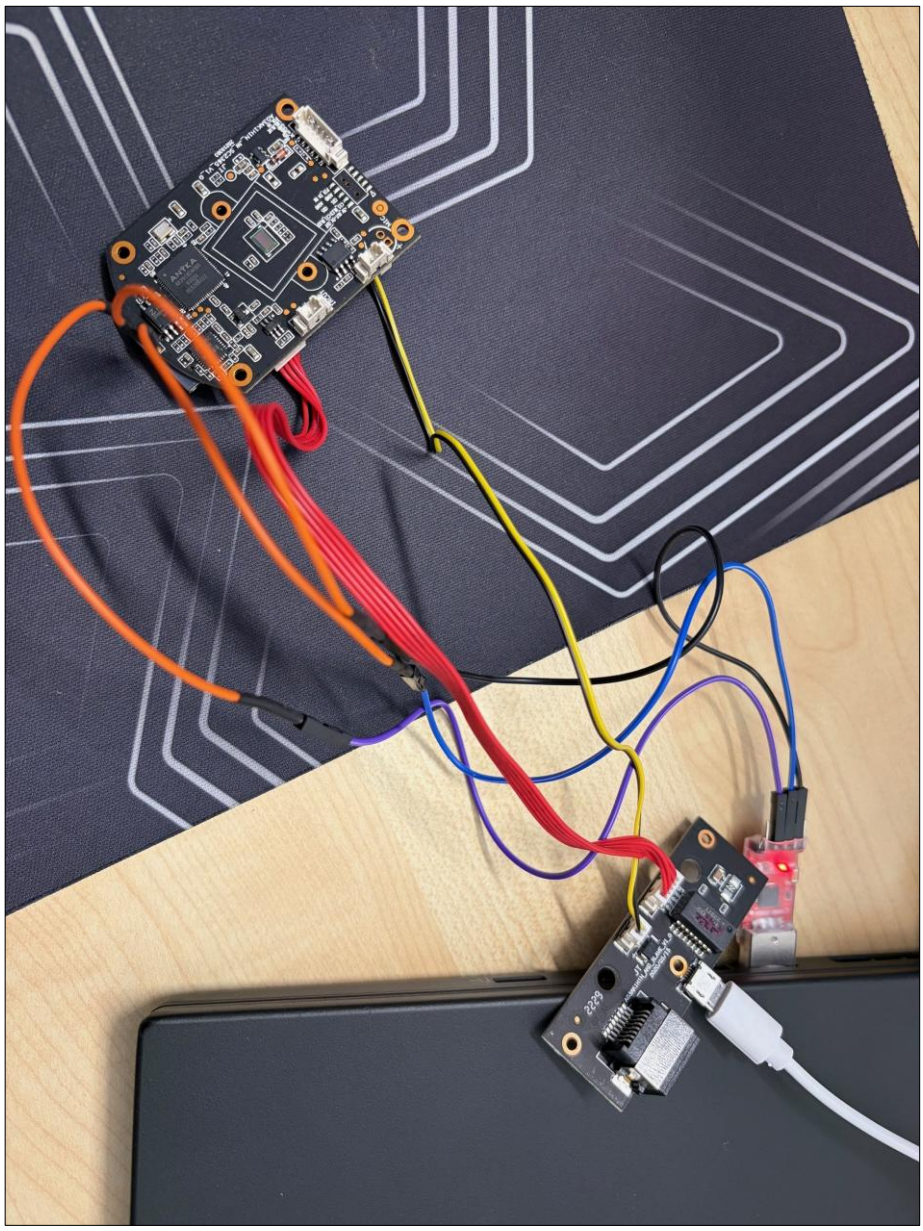
No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the component support remote sessions?	- A remote session is initiated when a component is accessed across the boundary of a zone defined by the asset owner based on their risk assessment.	Yes, the camera is controllable via the internet.	**N/A**
SL-C 2				
2.	Are remote sessions terminated either automatically after a reasonable timeframe of inactivity, manually by a local authority or manually by the user who initiated the session?	Yes.	Yes.	**PASS**

4.6.4 CR 2.13 – Use of Physical Diagnostic and Test Interfaces

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the host device provide a diagnostics or test interface?	- E.g. JTAG debugging	Yes, UART.	**N/A**
SL-C 2				
2.	Are physical factory diagnostics or test interfaces protected against unauthorized use?	Yes.	No, passwordless root login allowed.	**FAIL**

Details #2

For this test case the device was taken apart and a Serial to USB adapter was installed on the UART pins. This gave access to boot information as well as to the shell. For login there was not password needed. Providing the user name was enough.



```
$ sudo minicom -b 115200 -D /dev/ttyUSB0 -C capturefile
[CUT BY COMPASS]
VFS: Mounted root (squashfs filesystem) readonly on device 31:5.
devtmpfs: mounted
Freeing unused kernel memory: 140K
```

```
mount all file system...
starting mdev...
**********************
Love Linux ! ! !
**********************
Patch: The motor drive gpio is multiplexed with the gpio of uart1, and it is changed to
output at this time.
ak_uio: register uio device successfully with irq: 2!
set_pinctrl_vi pinctrl_lookup_state couldn't find csi0_sclk state
c2399_probe Apr 8 2021 13:55:36

[CUT BY COMPASS]
anyka login: root
[root@anyka ~]$ ls
bin etc lib mnt rom sys usr
dev ipc linuxrc proc sbin tmp var
[root@anyka ~]$
```

4.7 FR 3 - System Integrity

4.7.1 CR 3.1 – Communication Integrity

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Is the integrity of transmitted information protected?	Yes.	Yes.	**PASS**
SL-C 2				
2.	Is it possible to verify the authenticity of received information during communication?	Yes.	Yes.	**PASS**

4.7.2 CR 3.3 - Security Functionality Verification

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Is it regularly verified whether implemented security functions work as expected?	Yes.	Could not be evaluated.	**FAIL**
2.	Is there a process so that anomalies regarding security functions are reported during FAT, SAT or scheduled maintenance?	Yes.	Could not be evaluated.	**FAIL**

4.7.3 CR 3.4 – Software and Information Integrity

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Is it possible to perform integrity checks on software, configuration and other information as well as recording and reporting the results of these checks?	Yes. Either by the component itself or by another system.	Yes.	**PASS**
SL-C 2				
2.	Is it possible to perform authenticity checks on software, configuration and other information as well as recording and reporting the results of these checks?	Yes. Either by the component itself or by another system.	Yes.	**PASS**

4.7.4 CR 3.5 - Input Validation

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Is all input data validated in terms of syntax, length and content?	Yes.	Yes.	**PASS**

4.7.5 CR 3.6 – Deterministic Output

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the component physically or logically connect to an automation process?	-	No.	**N/A**

4.7.6 CR 3.7 – Error Handling

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Is information provided in error messages which could be exploited by attacker?	No.	No.	**PASS**

4.7.7 CR 3.8 – Session Integrity

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 2				
1.	Can sessions be invalidated upon user logout or other session termination?	Yes.	Yes.	**PASS**
2.	Are session identifiers unique and are only system-generated identifiers recognized?	Yes.	Yes.	**PASS**
3.	Are unique session identifiers created with commonly accepted sources of randomness?	Yes.	Yes.	**PASS**

4.7.8 CR 3.10 – Support for Updates

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Is it possible to update and upgrade the embedded device?	Yes.	Yes.	**PASS**
2.	If the embedded device is used for essential functions, can patches or upgrades be applied without impacting the essential functions?	Yes.	Not applicable.	**N/A**
SL-C 2				
3.	Is the authenticity and integrity of any update or upgrade validated before installation?	Yes.	Yes, the update / the new firmware is encrypted, and is decrypted on the device.	**PASS**

4.7.9 CR 3.14 – Integrity of the Boot Process

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Does the embedded device verify the integrity of the firmware, software and configuration data needed for the component's boot process prior to it being used in the boot process?	Yes.	No.	**FAIL**
SL-C 2				
2.	Does the host device use the component's supplier roots of trust to verify the authenticity of the firmware, software and configuration data needed in the boot process?	Yes.	In consequence of the above.	**FAIL**

Details #1

Boot log before:

```
[CUT BY COMPASS]
VFS: Mounted root (squashfs filesystem) readonly on device 31:5.
devtmpfs: mounted
Freeing unused kernel memory: 140K
mount all file system...
starting mdev...
**********************
Love Linux ! ! !
**********************
Patch: The motor drive gpio is multiplexed with the gpio of uart1, and it is changed to
output at this time.
ak_uio: register uio device successfully with irq: 2!
set_pinctrl_vi pinctrl_lookup_state couldn't find csi0_sclk state
c2399_probe Apr 8 2021 13:55:36
id:ffffff91
c2399_match fail
c3390_probe Jun 8 2021 11:44:38
id:ffffff91
[CUT BY COMPASS]
```

Boot log after modifying the firmware and flashing it back to ROM:

```
[CUT BY COMPASS]
VFS: Mounted root (squashfs filesystem) readonly on device 31:5.
devtmpfs: mounted
Freeing unused kernel memory: 140K
mount all file system...
starting mdev...
**********************
Love Compass ! !
**********************
Patch: The motor drive gpio is multiplexed with the gpio of uart1, and it is changed to
output at this time.
ak_uio: register uio device successfully with irq: 2!
set_pinctrl_vi pinctrl_lookup_state couldn't find csi0_sclk state
c2399_probe Apr 8 2021 13:55:36
id:ffffff91
c2399_match fail
c3390_probe Jun 8 2021 11:44:38
id:ffffff91
[CUT BY COMPASS]
```

4.8 FR 4 - Data Confidentiality

4.8.1 CR 4.1 – Information Confidentiality

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 1				
1.	Is the confidentiality of all data at rest for which explicit read authorization is supported protected?	Yes.	Yes.	**PASS**
2.	Is the confidentiality of data when traversing an untrusted network ensured?	Yes.	Yes.	**PASS**
3.	Is the confidentiality of information traversing any zone boundary protected?	Yes.	Yes.	**PASS**

4.8.2 CR 4.2 – Information Persistence

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
SL-C 2				
1.	Is sensitive data erased when it is being decommissioned?	Yes.	Yes, when the device has been hard reset.	**PASS**

5 Appendix

5.1 Compass Weaknesses Rating

Compass rates weaknesses based on their intrinsic technical properties. It should be noted that it is *not* a risk rating. Neither a threat actor's motivation (e.g., financial gain, fame, etc.) nor financial loss incurred by a successful exploitation of a weakness are taken into consideration.

All weaknesses are usually rated in isolation without considering the environment or any additional security controls that might be in place (i.e., vulnerabilities are rated in the context in which they are discovered).

A general description of each rating is given in the table below:

Rating	Description
Critical	▪ Successful exploitation has an immediate critical impact on the application/system: disclosure, manipulation or loss of sensitive data, elevation of privileges, disruption of service availability, etc. ▪ Exploitation does not require extensive effort, user interaction, elevated privileges, or combination with other complex or non-reliable exploits.
High	▪ Exploitation typically requires additional resources: user permissions, user interaction, large amounts of time/computing power, etc. ▪ Central security features & controls are turned off/not used ▪ Security-relevant processes or concepts are neither defined, nor implemented
Medium	▪ Exploitation typically requires significant effort and/or combination with other issues ▪ Security features & controls are implemented, but not configured according to best practices ▪ Security-relevant processes or concepts are defined, but important aspects are missing, unclear, or do not follow best practices
Low	▪ Exploitation typically leads to disclosure of information that is not sensitive but might be used in broader attack efforts (e.g., version information, user account names, etc.) ▪ Security features & controls are implemented with minor deviations from best practices ▪ Security-relevant processes or concepts are defined, but minor aspects are missing, unclear, or do not follow best practices
Info	▪ The entry is purely informational and has no security impact

The customer should review the individual weaknesses and their ratings and assign a risk score based on the company's risk management processes. Based on these risk scores, the customer should decide how and when the risk is handled (e.g., mitigate, accept, transfer, avoid).

5.2 Recheck Coloring

The following color code is used in rechecks to show the current state of a weakness:

Fixed	Partially Fixed	Not Fixed	New	Not Rechecked