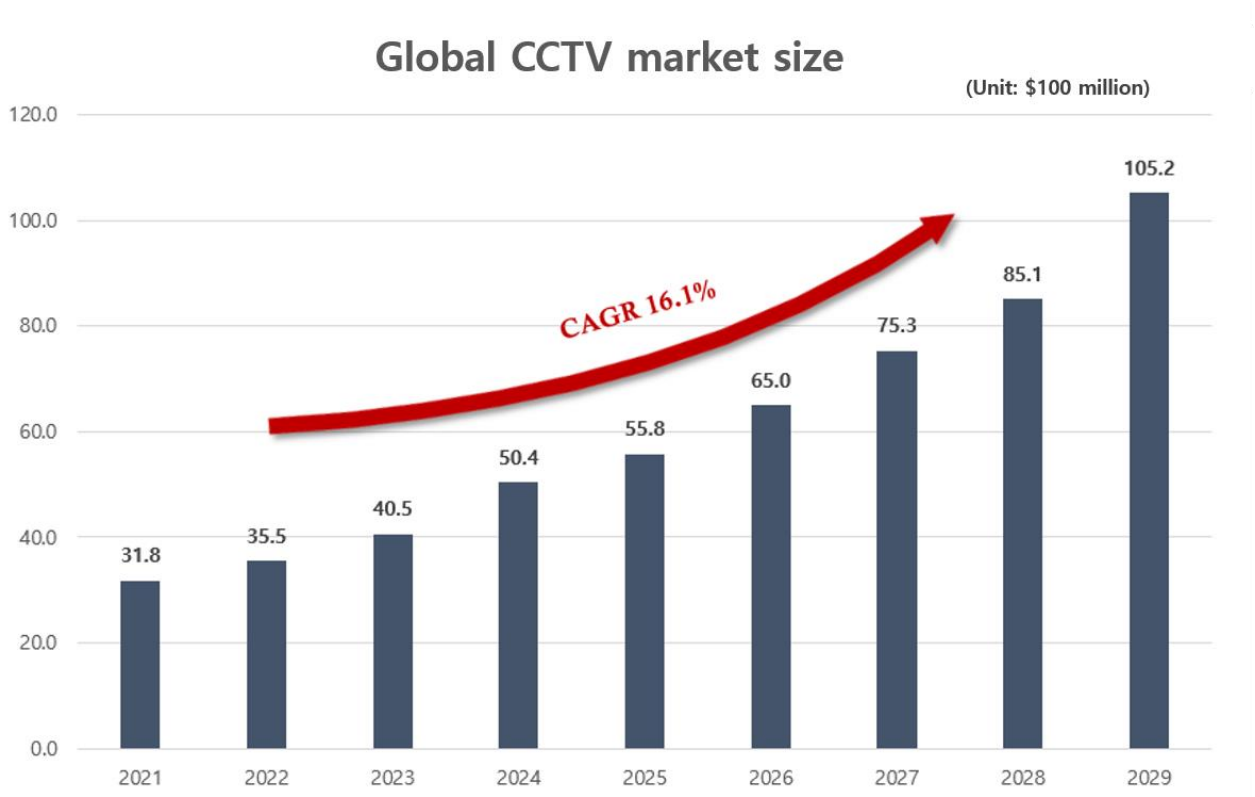
24/7 Watchdog: CCTV diagnosis uncovering invisible threats

■ CCTV security overview

The size of the global CCTV market is estimated to be $35.47 billion in 2022, showing an average annual growth rate of about 16%. It is expected to continue to grow and reach $105.2 billion in 2029. In particular, as CCTVs have become essential for preventing monitoring crimes and surveillance, and responding to potential safety threat factors in banks, financial institutions, public places, and industrial facilities, related demands are expected to continue to increase.



* Source: fortune business insights

Figure 1. Global CCTV market size[1]

[1] fortune business insights : https://www.fortunebusinessinsights.com/cctv-camera-market-107115

However, various security threats are occurring due to insufficient security awareness compared to the demand for more CCTVs. In 2016, there was a Mirai botnet[2] hacking incident in which major websites such as Twitter, Netflix, and New York Times were paralyzed by DDoS attacks targeting IoT devices including CCTVs. In addition, a series of actual damage cases occurred, e.g., the wallpad hacking incident (2022), in which the wallpads of about 400,000 households around the country were hacked, and private life videos were leaked through the built-in cameras, and the incident (2023), in which patients' treatment videos were leaked at a famous plastic surgery clinic in Gangnam. As we can easily find cases of cyberattacks through CCTV hacking around us, CCTV security is emerging as a popular social issue.

Accordingly, the need for CCTV security diagnosis is constantly emphasized. To prevent CCTV security incidents, it is necessary to check the overall security vulnerabilities of CCTVs from hardware to software and identify the risks and threat factors that may arise from them in advance.

SK Shieldus' EQST (Experts, Qualified Security Team) Group went further from web and mobile vulnerability diagnosis, which are the major areas, and is conducting technical vulnerability diagnosis for IoT devices including CCTVs. Through this, it is possible to improve the safety of CCTVs and IoT devices by identifying security vulnerabilities and taking appropriate countermeasures.

[2] Mirai botnet: A type of botnet that infects Internet of Things (IoT) devices with malware so that hackers can freely control them on the network.

■ EQST Group CCTV diagnosis criteria

The EQST Group of SK Shieldus has established its own CCTV diagnosis criteria by referring to the criteria if EQST IoT Diagnosis Guide v2.0.

No.	Classification	EQST security review diagnosis items	Web	Terminal	KISA IoT-SAP criteria
1	Hardware protection	Existence of physical interface	-	O	Whether external interface is deactivated and the access control function is provided if necessary Prevention unauthorized persons from accessing internal ports
2		Whether to the disassembly confirmation mechanism is applied	-	O	Whether to the function to detect and respond to unauthorized persons' tampering is provided
3		Whether firmware extraction is possible	-	O	-
4	Terminal protection	Whether to the OS alteration detection function is applied	-	O	Whether the reliable environment execution of remote control is inspected
5		Verification of the integrity of the firmware	-	O	Whether the integrity verification function is provided for key settings and exec codes Whether the integrity test is performed before updates
6		Whether the source codes are obfuscated	-	O	Whether source codes are obfuscated
7		Whether important information is stored in the terminal	-	O	Whether the important information stored in the product is encrypted
8		Whether important information is exposed in the memory	-	O	-
9		Whether important information in the screen is exposed in plain text	-	O	Whether the authentication information screen exposure is prevented and masked
10		Whether operation information is exposed in the app source codes	-	O	-
11		Whether important information is exposed in the debug log	-	O	-
12	Service protection	SQL injection	O	-	-
13		Malware upload	O	O	Whether secure coding is applied
14		Whether unsuitable users are authorized	O	O	Whether authorized users are checked before update
15		File download	O	-	-
16		Whether system operation information is exposed by external sites	O	-	-
17		Execution of OS commands	O	O	Whether secure coding is applied
18		XML external object attack (XXE)	O	-	-
19		Phishing attacks using the redirect function	O	-	-
20		LDAP injection	O	-	-
21		SSI injection	O	-	-
22		Insufficient user authentication	O	O	Whether identification and authentication for user identity verification precedes administration service and access to important information
23		Automation attack	O	O	Whether repeated authentication attempts are made through wrong authentication information
24		Buffer overflow attack	O	O	Whether secure coding is applied

Figure 2. EQST Group CCTV diagnosis criteria

The EQST Group established the EQST CCTV diagnosis criteria consisting of a total of 56 items by adding 39 items of the KISA diagnosis criteria and the items in the IoT-specific areas "service protection", "hardware protection", and "terminal security" areas. As a result of CCTV security inspection based on the criteria, it was found that the vulnerabilities of "hardware protection" and "service protection" items were the highest among security inspection items.

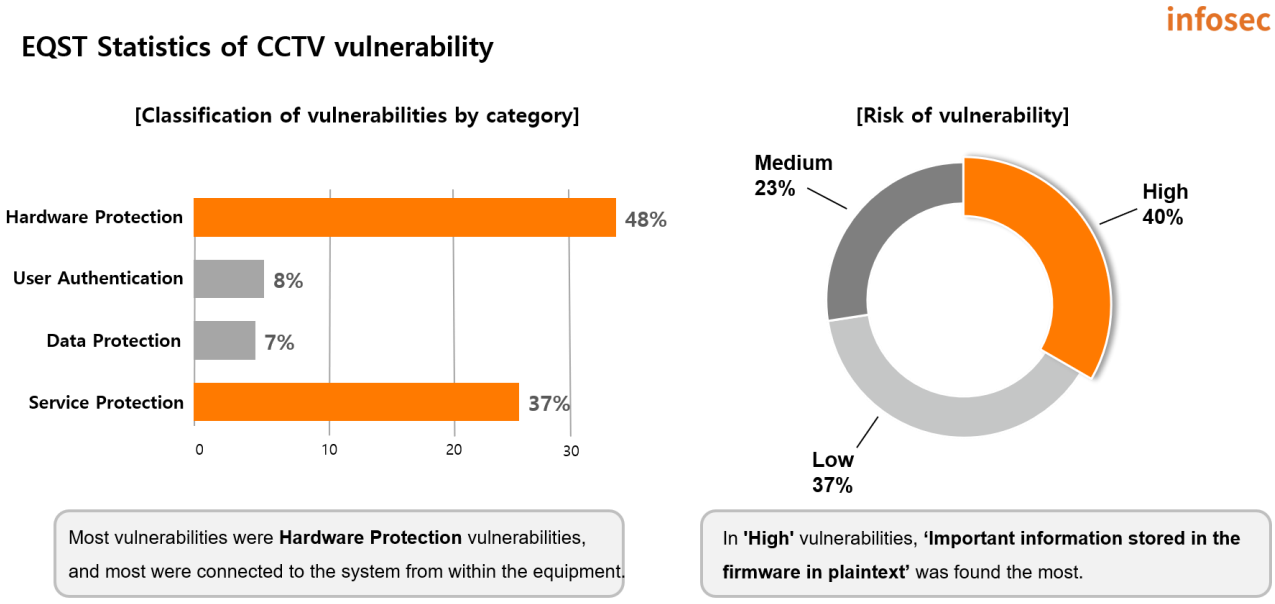


Figure 3. EQST Group CCTV diagnosis statistical table

■ EQST Group CCTV diagnosis process

The CCTV device diagnosis process carried out by the EQST Group is as follows:

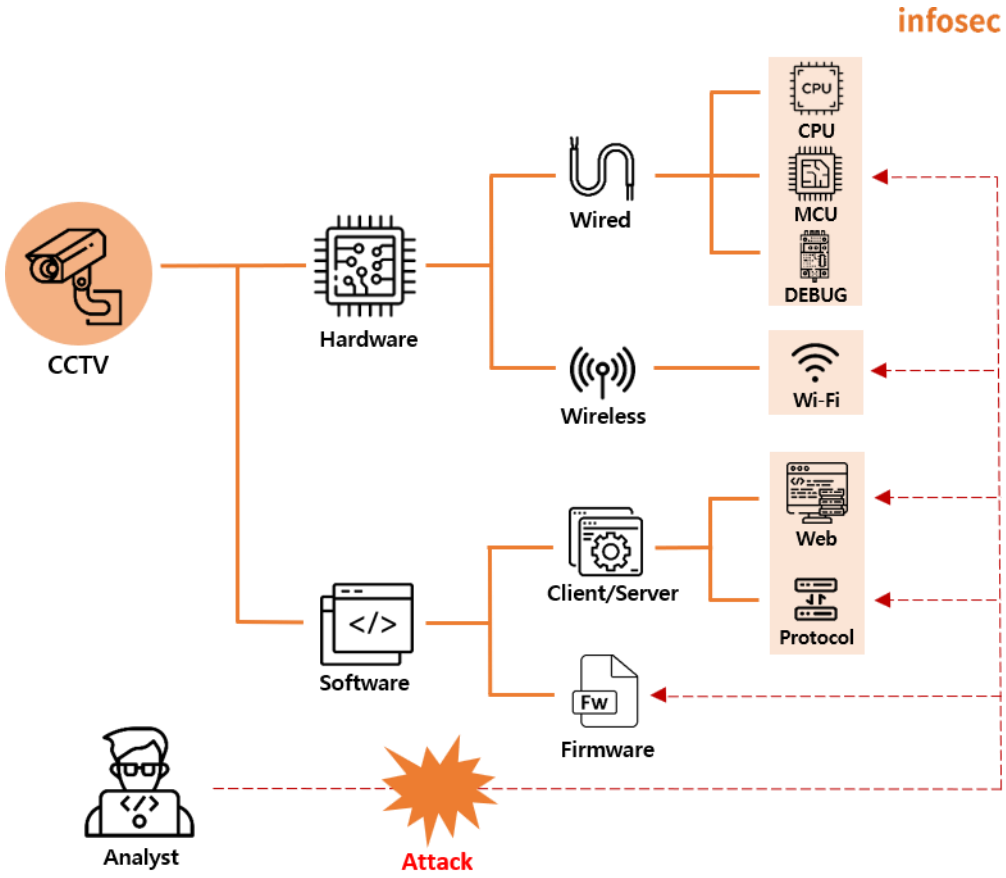


Figure 4. EQST Group's CCTV diagnosis process blueprint

The CCTV diagnosis area can be classified into hardware and software. Hardware is an area that diagnoses modules identified inside the device, and software is an area that diagnoses the programs of CCTV (IP Camera) devices or linked programs (example: lighttpd, Apache).

In the hardware area, threat elements for overall hardware are identified, e.g., whether a disassembly confirmation mechanism that can identify physical access to the inside of the device is applied, and whether important information (firmware, account information, secret keys, etc.) is exposed from the device's external interface.

The software area diagnoses authentication, authorization, and integrity areas for the platform through analysis and modification of the firmware extracted from the hardware. In addition, if there is an external management solution such as a client-server program associated with the device, a relevant solution is added in the CCTV diagnosis area, and the vulnerability linked to the device is checked.

■ CCTV attack surface analysis

In the past, CCTV was defined as a device that transmits video information on a closed network. However, most CCTVs today are open to the outside world as wired/wireless functions are used for efficient management or convenient accessibility improvement. Accordingly, management of diversified attack surfaces has become more important for CCTV security.

Below is a table that classifies the attack surface of CCTVs into four areas.

Area	Attack surface
Hardware protection	MCU, ROM[3], debug port
Service protection	Web services, mobile services, and other network services
User authentication	User authentication information
Data protection	Wired and wireless communication protocols, and encryption algorithms

1) Hardware protection

Unlike general systems, CCTVs are characterized by mass production and supply at low cost. As a result, the difficulty of acquiring the same product is relatively low. Such low-cost mass production requires attention because it is possible to analyze the device's operating system or service through an alternative terminal even if the attacker does not directly access the installed terminal.

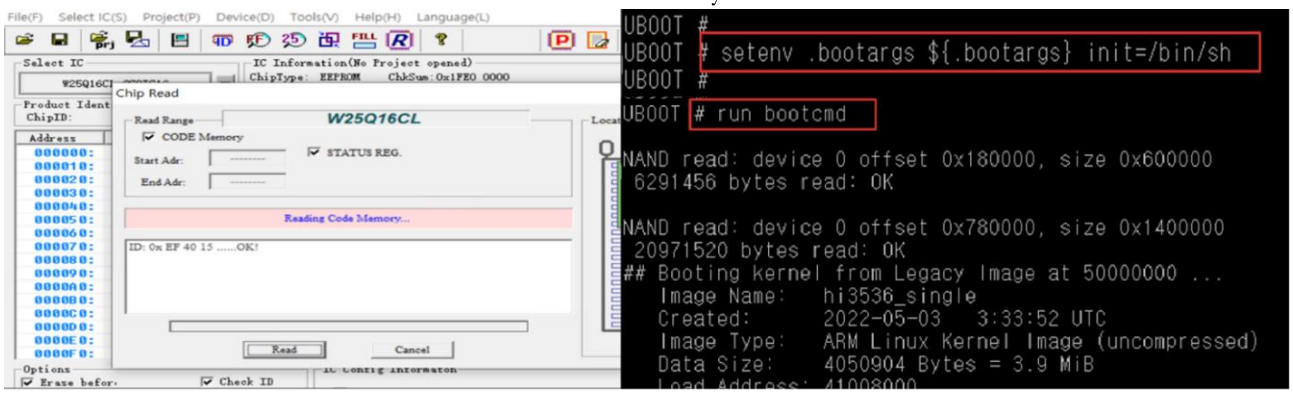


Figure 5. Extraction of firmware using the MCU chip

The microcontroller unit (MCU) visually identifies the flash memory in which the firmware is stored, extracts the firmware, and tries to enter[4] the device boot loader through the debug interface[5]. At this time, if there is no special security setting, it is possible to easily acquire the boot loader command shell. As vulnerabilities identified in the process can act effectively on devices in actual operation, hardware checks must be inspected.

[3] ROM: A non-volatile storage device for storing data (example: EMMC, Flash memory)

[4] Device boot loader entry: A booting code used to run OS exclusively for IoT (example: PC CMOS)

[5] Debug interface: A non-volatile storage device for storing data (example: EMMC, Flash memory)

2) Service protection

Recently, with the development of technology, it is possible to easily and conveniently use various network services, such as remote viewing and management of CCTV images through web services and mobile apps. However, if it is possible to access CCTVs through a mobile app, caution is required as it can take over the user's device by attacking the vulnerability of the linked app itself.

Figure 6. CVE analysis through web server version information

The attacker can acquire internal information of the system through the information left in the web server development stage and the error page set as default in the server. Furthermore, if information about the web server version is exposed, as an attack using CVE (Common Vulnerabilities and Exposure) becomes possible for that version, it can lead to high-risk infringement incidents such as video information leakage. Therefore, if there is a service that interfaces with CCTVs, it is necessary to check it and take measures by applying the latest patches and security updates to all related elements.

3) User authentication

If the API key or administrator account information used for CCTV operation is exposed without being encrypted in the firmware or device, an attacker can use the information to manipulate the device or obtain administrator privilege. In addition, you need to be careful because the attacker can attempt an attack by entering the default account information for the administration webpage and access the system based on the authentication information found. In fact, malware such as Mirai and Mozi perform attacks by brute-forcing authentication information and default account information commonly used in CCTVs to infect an unspecified number of IoT devices.

```
class DictionaryAttack:
    def __init__(self, password=str):

        self.password = password
        self.password_hash = hashlib.sha256(password.encode()).hexdigest()

        self.success = "The password was found: "
        self.fail = "The password could not be cracked "

    def crack_password(self):

        with open(
            r"yourpath", "r",
            encoding="latin-1") as f:
            words = f.read().split()

            for word in words:
                word_hash = hashlib.sha256(word.encode()).hexdigest()

                if word_hash == self.password_hash:
                    return self.success + self.password
            else:
                return self.fail
```

Sn.	CCTV Company	Default Username	Default Password	Default IP Address
1	Hikvision	admin	12345	192.0.0.64
2	TVT	admin	123456	192.168.226.1
3	Sony	admin	admin	192.168.0.100
4	Samsung	root	4321 or admin	192.168.1.200
5	Samsung	admin	4321 or 1111111	192.168.1.200
6	FLIR	admin	fliradmin	192.168.250.116
7	Avigilon	admin	admin	no default/DHCP
8	Panasonic	admin	12345	192.168.0.253
9	Panasonic	admin1	password	192.168.0.253
10	ACTi	Admin or admin	123456	192.168.0.100
11	Axis	root	pass or no set password	192.168.0.90
12	Bosch	service	service	192.168.0.1
13	Bosch	Dinion	no set password	192.168.0.1
14	Vivotek	root	no set password	no default/DHCP
15	Arecont Vision	admin	no set password	no default/DHCP
16	Honeywell	administrator	1234	no default/DHCP

Figure 7. Dictionary attack and initial account information by manufacture

* Source: cctvdesk[6]

For many IoT devices, including CCTVs, basic account information set at the time of shipment can be found through manuals provided by manufacturers or on the Internet. Therefore, the best way to prevent brute force attacks is to change the default password. Currently, many manufacturers are making it mandatory to reset the password when logging in for the first time to enhance security. When setting a password, users should be more careful to maintain a high level of security by making efforts not to use consecutive letters or numbers and not use words in the dictionary as they are.

[6] cctvdesk : https://cctvdesk.com/cctv-default-password/

4) Data protection

When transmitting and receiving important data, such as CCTV images, through an unsafe channel, hackers may peep or tamper with it. So care must be taken. In addition, even though an encryption protocol is used, if a vulnerable encryption protocol is used, communication data can be intercepted and forcibly decrypted. So the encryption algorithm must be checked as well. Therefore, it is important to prevent data by using an encryption protocol with high reliability and strength in wired/wireless communication.

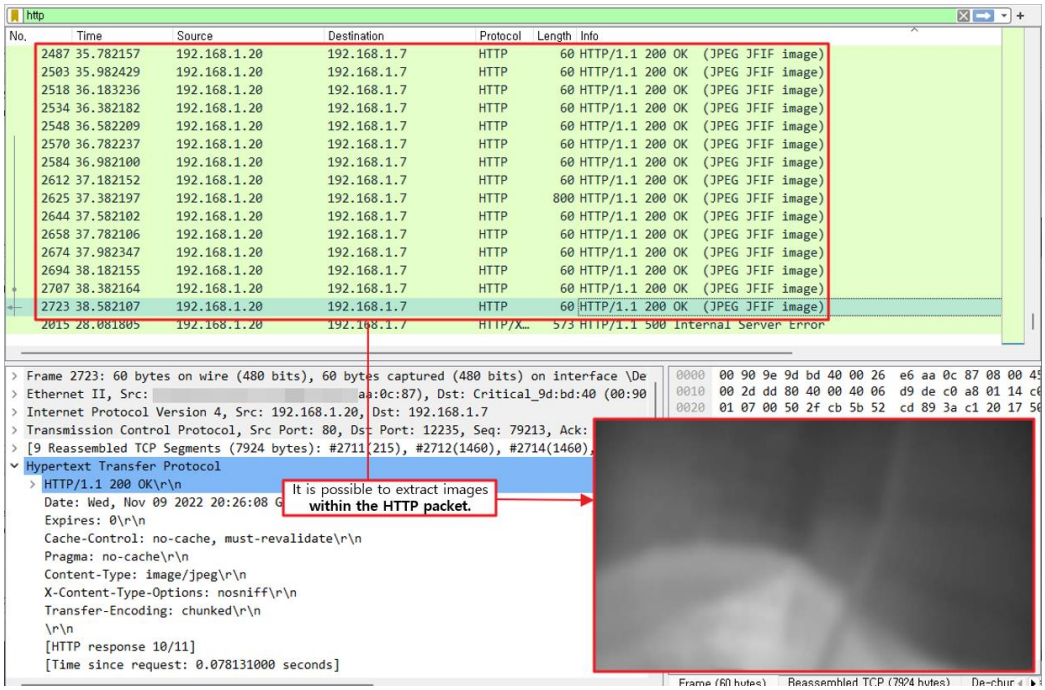


Figure 8. Exposure of plain-text image information within the HTTP protocol

For example, when CCTV device image data is transmitted with the HTTP protocol[7], it will be possible to arbitrarily extract the protocol image using the MITM[8] technique. Distributing the image data may cause direct or indirect damage. Therefore, for the security of CCTV video data, it is necessary to conduct self-encryption using a safe encryption algorithm other than vulnerable encryption algorithms like MD5[9] and RC4[10], or apply SSL encryption to the protocol before transmission.

[7] HTTP protocol: A protocol that follows the server/client model for exchanging data on the Internet

[8] MITM: Man in the Middle, an attack in which an attacker intercepts data transmission by intervening between the user's Internet server and the destination of the Internet traffic

[9] MD5: It is a 128-bit encryption hash function. It is recommended not to use it due to a design defect in 1996.

[10] RC4: RC4 is a stream cipher developed by Ron Rivest of RSASecurity in 1987 and has been the standard encryption protocol of SSL since 1995.

■ Closing

With the recent increase in demand for CCTVs and IoT, various wired and wireless functions are added to secure connectivity, convenience, and availability between users. However, cyber attacks and issues exploiting vulnerabilities in wired/wireless functions are constantly occurring, and in order to respond to these threats, companies and users need to pay attention to CCTV and IoT security incidents and make efforts to diagnose vulnerabilities.

In order to respond to cyber attacks using CCTVs and IoT, the EQST Group has established its own IoT diagnosis standards and is conducting inspections, and is continuously upgrading by revising the diagnosis standards according to changes in trends. For detailed information, see the EQST IoT Diagnosis Guide v.2.0.

[Link] Shortcut to full text download: IoT Diagnosis Guide 2.0 proposed by the EQST Group

■ Reference sites

url: https://www.lighttpd.net/

url: https://www.fortunebusinessinsights.com/cctv-camera-market-107115

url: https://github.com/DataBach-maker/DictionaryAttackExample

url: https://cctvdesk.com/cctv-default-password/

url: https://book.hacktricks.xyz/network-services-pentesting/554-8554-pentesting-rtsp

url: https://www.wowza.com/community/t/encrypting-an-rtsp-stream/36108