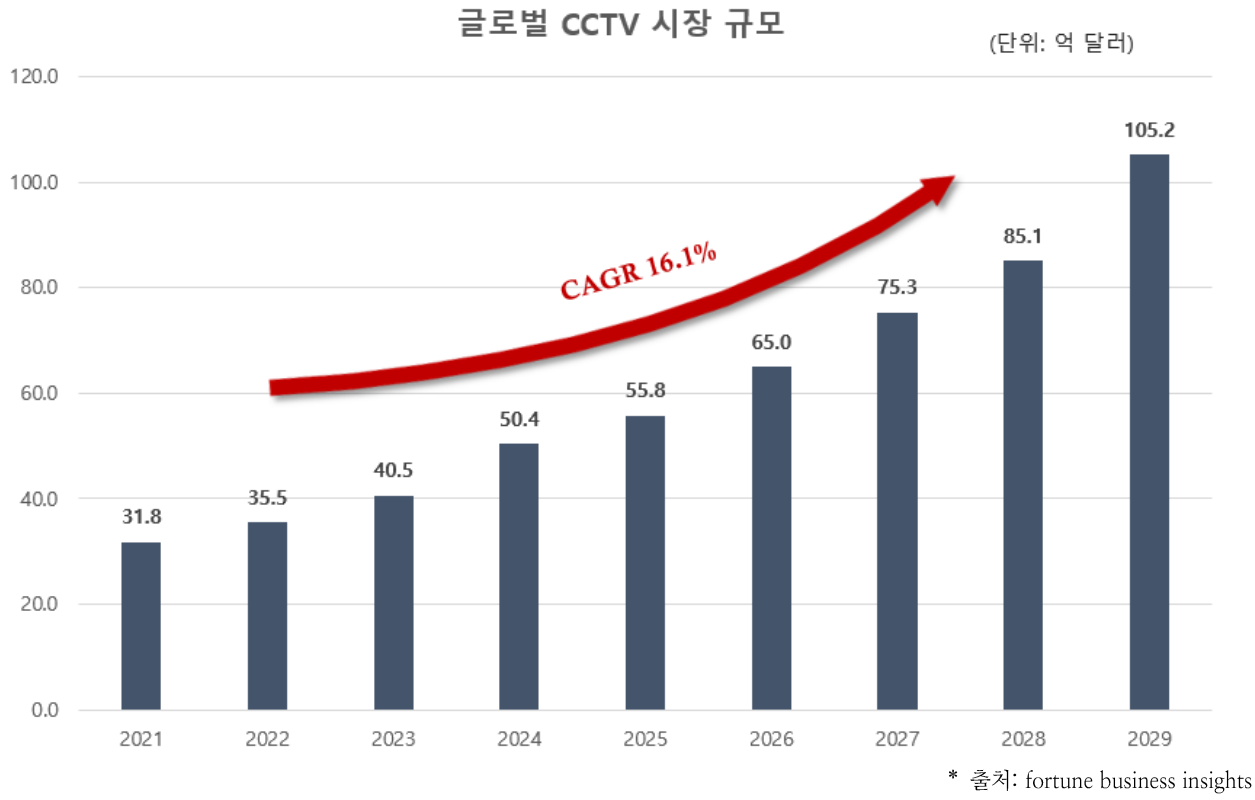
24/7 Watchdog: 보이지 않는 위협을 밝히는 CCTV 진단

■ CCTV 보안 개요

전 세계 CCTV 시장 규모는 2022 년 354 억 7,000 만 달러로 추산되며, 연 평균 약 16%의 성장률을 보이고 있다. 앞으로도 지속적으로 성장해 2029 년에는 1,052 억 달러 규모에 달할 것으로 예상된다. 특히 CCTV 가 은행, 금융기관, 공공장소, 산업시설에서 범죄 예방 및 감시, 잠재적 안전 위협 요인 대응을 위한 필수품으로 자리매김하면서 관련 수요는 지속적으로 증가할 전망이다.



* 출처: fortune business insights

그림 1. 글로벌 CCTV 시장 규모 그래프[1]

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

그러나, CCTV 증가 수요 대비 부족한 보안 인식으로 인해 각종 보안 위협이 발생하고 있다. 2016 년에는 CCTV 를 비롯한 IoT 기기를 대상으로 디도스 공격을 감행하여 트위터, 넷플릭스, 뉴욕타임즈 등 주요 웹사이트가 마비된 미라이 봇넷[2] 해킹 사건이 발생한 바 있으며, 이외에도 국내 전국 약 40 만가구의 월패드가 해킹되어 내장된 카메라를 통해 사생활 영상이 유출되었던 월패드 해킹 사건(2022년), 강남 유명 성형외과에서 환자들의 시술 영상이 유출된 사건(2023년) 등 실제 피해 사례가 잇따라 발생했다. 이처럼 우리 주변에서 어렵지 않게 CCTV 해킹을 통한 사이버공격 사례를 찾아볼 수 있게 되면서 CCTV 보안이 대중적인 사회 이슈로 떠오르고 있다.

이에 따라 CCTV 보안 진단에 대한 필요성이 끊임없이 강조되고 있다. CCTV 보안 사고를 막기 위해서는 하드웨어부터 소프트웨어까지 CCTV 에 대한 전반적인 보안 취약성을 점검하고 이로 인해 발생할 위험과 위협 요인을 사전에 파악해야 한다.

SK 쉴더스의 EQST(이큐스트, Experts, Qualified Security Team) 그룹에서는 주요 영역인 웹, 모바일 취약점 진단에서 더 나아가 CCTV 를 포함한 IoT 디바이스를 대상으로 기술적 취약점 진단을 수행하고 있다. 이를 통해 보안 취약성을 식별하고 적절한 대응 조치를 취함으로써 CCTV 와 IoT 디바이스의 안전성을 향상시킬 수 있다.

[2] 미라이 봇넷: 사물인터넷(IoT) 기기를 악성코드에 감염시켜 네트워크상에서 해커가 마음대로 제어할 수 있게 하는 봇넷(Botnet)의 일종

■ EQST 그룹 CCTV 진단 기준

SK 쉴더스 EQST 그룹은 EQST IoT 진단 가이드 v2.0 기준을 참고하여 자체 CCTV 진단 기준을 수립하여 진행하고 있다.

NO.	구분	자사 보안성심의 진단항목	웹	단말	KISA 사물인터넷 보안인증(IoT-SAP) 기준
1	하드웨어 보호	물리적 인터페이스 존재 여부	-	O	외부 인터페이스 비활성화, 필요시 접근통제 기능 제공 여부 비인가자의 내부 포트 접근 방지
2		분해 확인 매커니즘 적용 여부	-	O	비인가자의 무단 조작 탐지 및 대응 기능 제공 여부
3		펌웨어 추출 가능 여부	-	O	-
4	단말보안	OS 변조 탐지 기능 적용 여부	-	O	원격관리의 신뢰할 수 있는 환경 실행 검사 여부
5		펌웨어 무결성 검증	-	O	주요 설정 값 및 실행코드에 무결성 검증기능 제공 여부 업데이트 수행 전 무결성 검사 수행 여부
6		소스코드 난독화 적용 여부	-	O	소스코드 난독화 적용 여부
7		단말기 내 중요정보 저장 여부	-	O	제품에 저장되는 중요정보 암호화 여부
8		메모리 내 중요정보 노출 여부	-	O	-
9		화면 내 중요정보 평문 노출 여부	-	O	인증정보 화면 노출 방지 및 마스킹 적용 여부
10		앱 소스코드 내 운영정보 노출 여부	-	O	-
11		디버그 로그 내 중요정보 노출 여부	-	O	-
12	서비스 보호	SQL Injection	O	-	-
13		악성파일 업로드	O	O	시큐어코딩 적용 여부
14		부적절한 이용자 인가 여부	O	O	업데이트 수행 전 인가된 사용자 확인 여부
15		파일 다운로드	O	-	-
16		외부사이트에 의한 시스템 운영정보 노출 여부	O	-	-
17		운영체제 명령실행	O	O	시큐어코딩 적용 여부
18		XML 외부객체 공격 (XXE)	O	-	-
19		리다이렉트 기능을 이용한 피싱 공격	O	-	-
20		LDAP Injection	O	-	-
21		SSI Injection	O	-	-
22		불충분한 이용자 인증	O	O	관리서비스 및 중요정보 접근 시 사용자 신원 검증 위한 식별 및 인증 선행 여부 제품 간 중요정보 전송 시 제품 제어를 위한 상호연결 수행 시 상호 인증 선행 여부
23		자동화공격	O	O	잘못된 인증정보 통한 반복 인증 시도 제한 여부
24		버퍼오버플로우 (Buffer Overflow Attack)	O	O	시큐어코딩 적용 여부

그림 2. EQST 그룹 CCTV 진단 기준

EQST 그룹은 KISA 진단 기준 39 개 항목과 함께 IoT 특화 영역인 “서비스 보호”, “하드웨어 보호”, “단말 보안” 영역의 항목을 중점적으로 추가하여 총 56 개의 항목으로 구성된 EQST CCTV 진단 기준을 수립했다. 해당 기준을 기반으로 CCTV 보안 점검을 수행한 결과, 보안 점검 항목 중 “하드웨어 보호”, “서비스 보호” 항목의 취약점이 가장 높은 것으로 나타났다.

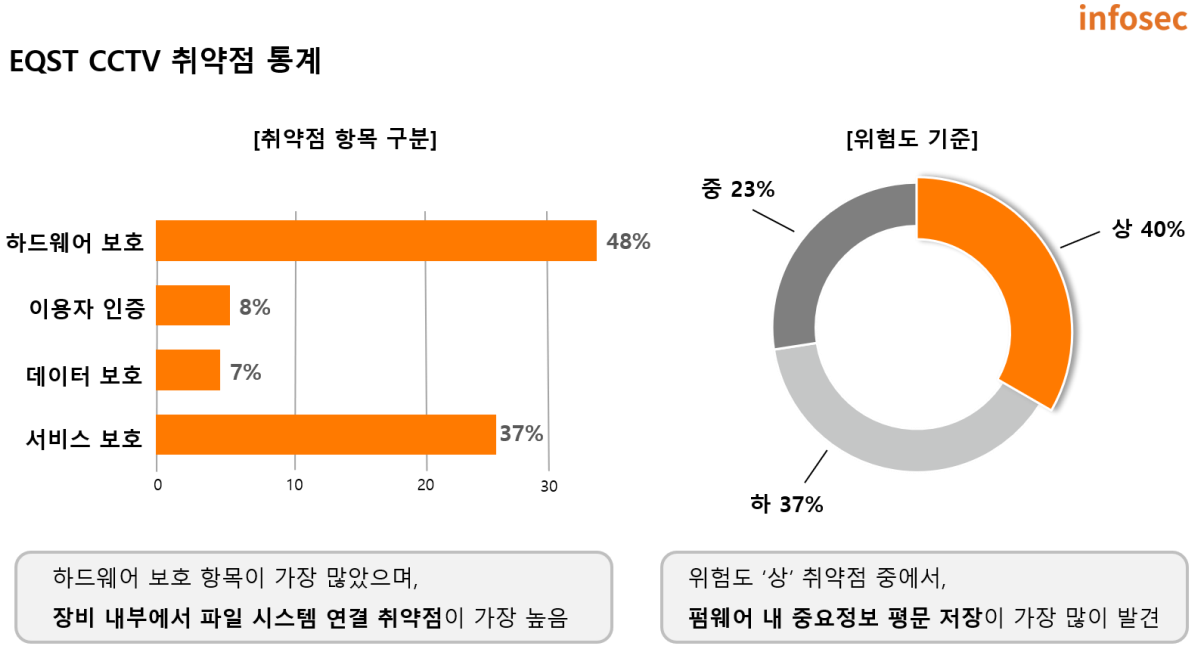


그림 3. EQST 그룹 CCTV 진단 통계표

■ EQST 그룹 CCTV 진단 프로세스

EQST 그룹에서 진행하고 있는 CCTV 디바이스 진단 프로세스는 아래와 같다.

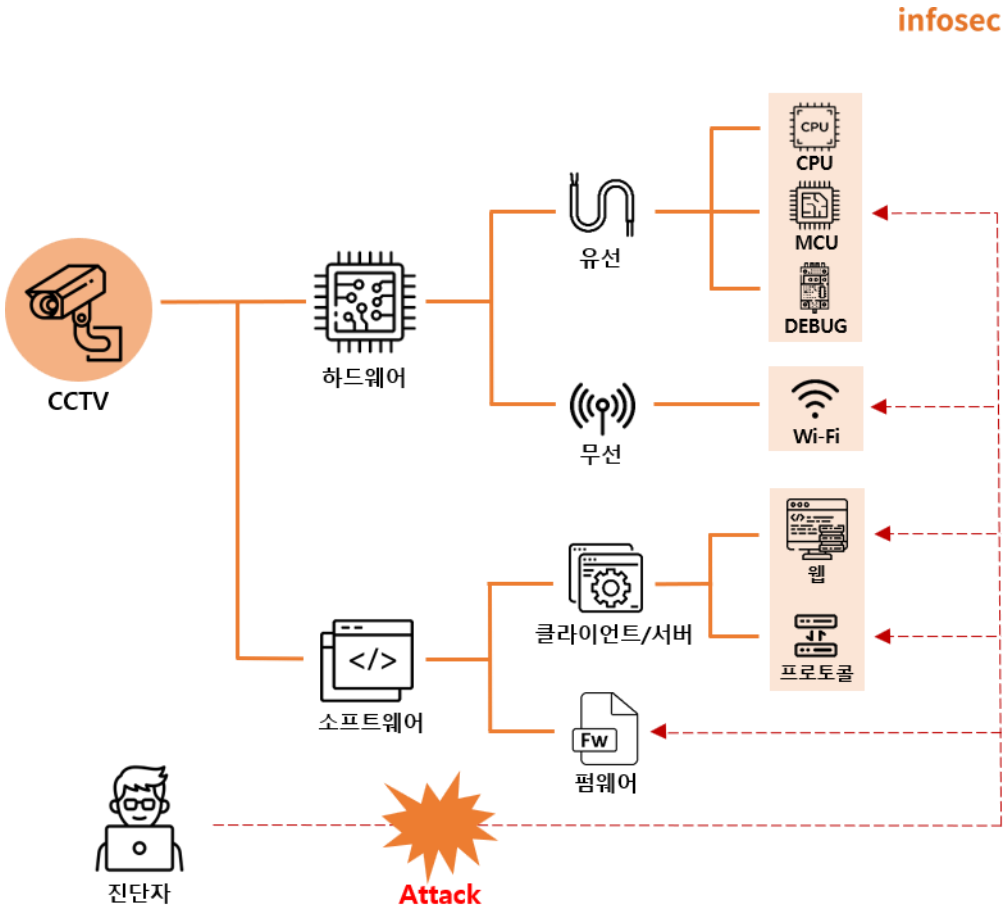


그림 4. EQST 그룹의 CCTV 진단 프로세스 설계도

CCTV 진단 영역은 하드웨어와 소프트웨어로 분류할 수 있다. 하드웨어는 디바이스 내부에 식별되는 모듈을 진단하는 영역이며, 소프트웨어는 CCTV(IP Camera) 디바이스 자체 프로그램 또는 연계 프로그램(예: lighttpd, Apache)을 진단하는 영역이다.

하드웨어 영역에서는 디바이스 내부에 대한 물리적인 접근 여부를 식별할 수 있는 분해 확인 메커니즘 적용 여부, 디바이스 외부 인터페이스로부터 중요 정보(펌웨어, 계정 정보, 비밀 키 등) 노출 여부 등 하드웨어 전반에 대한 위협 요소들을 식별한다.

소프트웨어 영역은 하드웨어에서 추출한 펌웨어를 분석 및 변조를 통해 플랫폼에 대한 인증, 인가, 무결성 영역 등을 진단한다. 또한 디바이스와 연계된 클라이언트-서버 프로그램 등 외부 관리 솔루션이 존재하는 경우, CCTV 진단 영역 내 해당 솔루션을 추가하여 디바이스와 연계한 취약점을 점검한다.

■ CCTV 공격 표면 분석

과거 CCTV 는 폐쇄적인 망에서 영상정보를 송신하는 역할을 수행하는 기기로 정의됐다. 하지만 오늘날 대부분의 CCTV 는 효율적인 관리나 편리한 접근성 개선 등을 위해 유무선 기능을 사용함에 따라 외부에 공개되어 있다. 따라서 CCTV 보안을 위해서는 다각화된 공격 표면에 대한 관리가 더욱 중요해졌다.

아래는 CCTV 의 공격 표면을 크게 네 가지의 영역으로 분류한 표다.

영역	공격 표면
하드웨어 보호	MCU, ROM[3], 디버그 포트
서비스 보호	웹 서비스, 모바일 서비스, 기타 네트워크 서비스
이용자 인증	사용자 인증 정보
데이터 보호	유무선 통신 프로토콜, 암호화 알고리즘

1) 하드웨어 보호

CCTV 는 일반적인 시스템과는 달리 저비용으로 대량 생산 및 공급되는 특성을 가지고 있다. 이로 인해 동일한 제품을 입수하기 위한 난이도가 비교적 낮다. 이러한 저비용 대량 생산은 공격자에게 설치된 단말기에 직접 접근하지 않더라도 대체 단말기를 통해 기기의 운영체제나 서비스에 대한 분석이 가능해 주의가 필요하다.

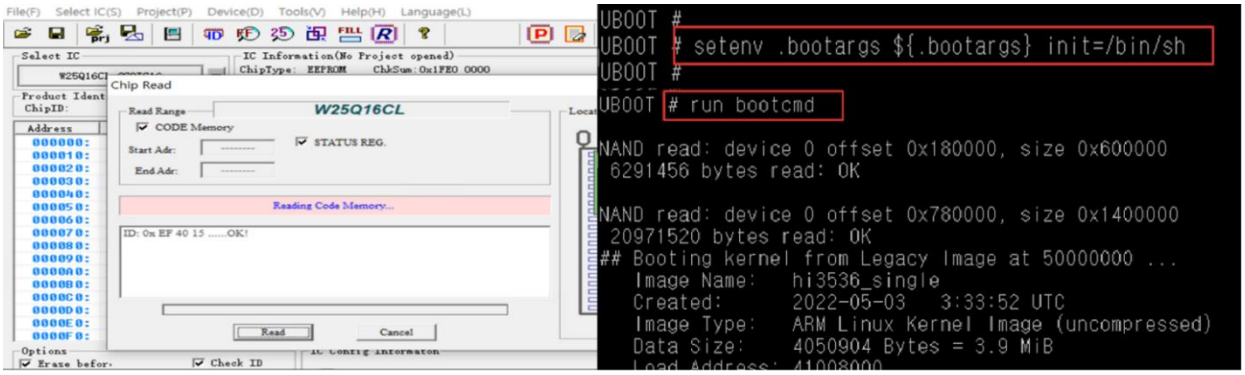


그림 5. MCU 칩을 이용한 펌웨어 추출

마이크로컨트롤러(MicroController Unit, MCU)에서 펌웨어가 저장된 플래시 메모리를 육안으로 식별하고 펌웨어를 추출하며 디버그 인터페이스[4]를 통하여 디바이스 부트 로더 진입[5]을 시도하게 된다. 이때, 별다른 보안 설정이 되어있지 않다면 쉽게 부트 로더 명령어 쉘 획득이 가능하다. 해당 과정에서 식별된 취약점은 실제 운영중인 기기에 유효하게 작용할 수 있으므로 하드웨어에 대한 점검은 반드시 이루어져야 한다.

---

[3] ROM : 데이터를 저장하기 위한 비휘발성 저장 장치(예: EMMC, Flash 메모리)

[4] 디버그 인터페이스 : 데이터를 저장하기 위한 비휘발성 저장 장치(예: EMMC, Flash 메모리)

[5] 디아비스 부트 로더 진입 : IoT 전용 OS 를 실행하기 위해 사용하는 부팅 코드(예: PC CMOS)

2) 서비스 보호

최근에는 기술 발전에 따라 웹 서비스와 모바일 앱을 통해 CCTV 영상 원격 조회 및 관리 등 쉽고 편리한 다양한 네트워크 서비스 이용이 가능하다. 다만, 모바일 앱을 통해 CCTV 에 접근이 가능한 경우, 연동 앱 자체의 취약점을 공격하여 사용자의 디바이스를 장악할 수 있어 주의가 필요하다.

그림 6. 웹 서버 버전 정보를 통한 CVE 분석

공격자는 웹 서버 개발 단계에서 남겨진 정보와 서버 내 디폴트로 설정되어 있는 에러 페이지 등을 통해 시스템의 내부 정보 획득이 가능하다. 더욱이 웹 서버 버전에 대한 정보가 노출될 경우, 해당 버전에 대해 알려진 취약점(CVE)를 이용한 공격이 가능해져 영상 정보 유출 등 높은 위험의 침해 사고가 발생할 수 있다. 따라서 CCTV 와 연동되는 서비스가 있다면 이와 관련한 모든 요소에 대해 최신 패치와 보안 업데이트 등을 적용한 점검 및 조치가 필요하다.

3) 이용자 인증

CCTV 동작에 사용되는 API 키나 관리자 계정 정보가 펌웨어 혹은 기기 내에 암호화되지 않은 채 노출되어 있다면, 공격자는 해당 정보를 이용해 기기를 조작하거나 관리자 권한을 획득할 수 있다. 또한, 관리 웹페이지에 대한 디폴트 계정 정보를 대입하여 공격을 시도하고 알아낸 인증 정보를 기반으로 시스템에 접근할 수 있어 주의가 필요하다. 실제로 Mirai, Mozi 와 같은 악성코드들은 불특정 다수의 IoT 기기를 감염 시키기 위해 CCTV 에서 일반적으로 자주 사용되는 인증 정보와 디폴트 계정 정보 등을 무차별 대입하는 방식을 사용해 공격하고 있다.

```python
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

그림 7. 사전 대입 공격 및 제조사별 초기 계정정보

* 출처: cctvdesk[6]

CCTV 를 포함한 많은 IoT 장치는 공정 출하 시 설정되어 있는 기본 계정 정보를 제조사에서 제공하는 매뉴얼 또는 인터넷을 통해 찾을 수 있다. 따라서, 무차별 대입 공격을 방지하기 위한 가장 좋은 방법은 기본으로 설정되어 있는 암호를 변경하는 것이다. 현재는 많은 제조사들이 보안을 강화하기 위해 처음 로그인 시 비밀번호를 재설정하도록 의무화하고 있다. 사용자도 비밀번호를 설정할 때, 연속 문자나 숫자를 사용하지 않고 사전에 있는 단어를 그대로 사용하지 않는 등의 노력을 통해 높은 수준의 보안을 유지할 수 있도록 더욱 주의해야 한다.

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

4) 데이터 보호

CCTV 영상처럼 중요한 데이터를 안전하지 않은 채널을 통해 송수신 하는 경우, 해커가 이를 엿보거나 변조할 수 있어 주의가 필요하다. 또한, 암호화 프로토콜을 사용한다고 하더라도 취약한 암호화 프로토콜을 사용하는 경우, 통신 데이터를 가로채서 강제로 복호화 할 수 있기 때문에 암호화 알고리즘에 대한 점검도 함께 이루어져야 한다. 따라서 유무선 구간의 통신에서는 높은 신뢰성과 강도를 지닌 암호화 프로토콜을 사용해 예방하는 것이 중요하다.

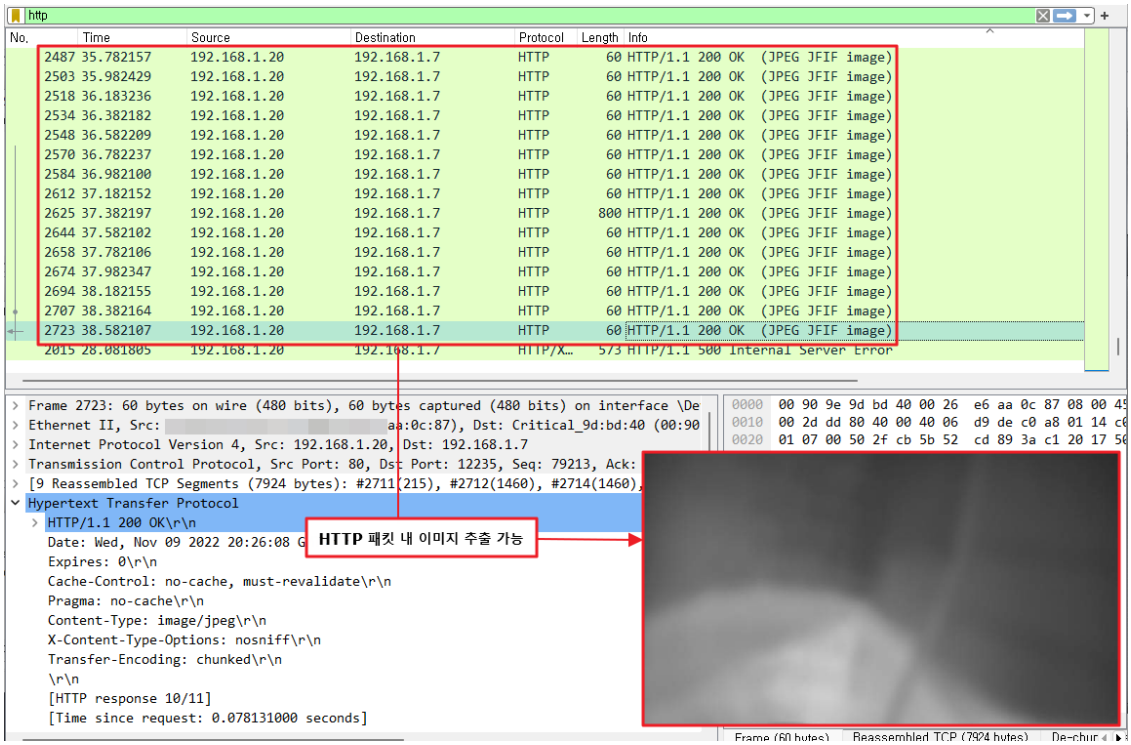


그림 8. HTTP 프로토콜 내 평문 영상정보 노출

예시로 CCTV 디바이스 영상정보를 HTTP 프로토콜[7]로 전송하는 경우, MITM[8] 기법을 이용하여 프로토콜 영상정보를 임의로 추출할 수 있게 된다. 해당 영상 정보를 유포하게 된다면 직간접적인 피해가 발생할 수 있다. 따라서 CCTV 영상 정보의 보안을 위해서는 MD5[9], RC4[10]등 취약한

[7] HTTP 프로토콜 : 인터넷상에서 데이터를 주고 받기 위한 서버/클라이언트 모델을 따르는 프로토콜

[8] MITM : Man in the Middle, 공격자가 사용자의 인터넷 서버와 해당 인터넷 트래픽의 목적지 사이에 끼어들어 데이터 전송을 가로채는 공격

[9] MD5 : 128 비트 암호화 해시 함수로 1996 년 설계상 결함이 발생하여 사용하지 않도록 권고됨

[10] RC4 : RC4는 1987년 RSA 시큐리티의 로널드 라이베스트(Ron Rivest)에 의해 개발된 스트림 암호로 1995 년부터 SSL의 표준 암호화 프로토콜

암호화 알고리즘을 제외한 안전한 암호화 알고리즘을 사용하여 자체 암호화를 진행하거나 프로토콜에 대한 SSL 암호화를 적용하여 전송해야 한다.

■ 맺음말

최근 CCTV 및 IoT 에 대한 수요 증가와 함께 사용 간의 연결성, 편의성, 가용성을 확보하고자 다양한 유무선 기능이 더해지고 있다. 그러나 유무선 기능의 취약점을 악용한 사이버 공격과 이슈가 끊임없이 발생하고 있고 있으며, 이러한 위협에 대응하기 위해서는 기업과 사용자들이 CCTV 및 IoT 보안 사고에 대한 관심을 갖고 취약점을 진단할 수 있는 노력이 필요하다.

EQST 그룹에서는 CCTV 및 IoT 를 이용한 사이버 공격에 대응하기 위해 자체적으로 IoT 진단 기준을 수립하여 점검을 진행하고 있으며, 트렌드 변화에 따라 진단 기준을 개정하여 지속적인 고도화를 진행하고 있다. 자세한 내용은 EQST IoT 진단 가이드 v.2.0 에서 확인할 수 있다.

[링크] 전문 다운로드 바로가기: EQST 그룹이 제안하는 IoT 진단가이드 2.0

■ 참고사이트

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