infosec

Threat Intelligence Report

EQST INSIGHT

2023

07

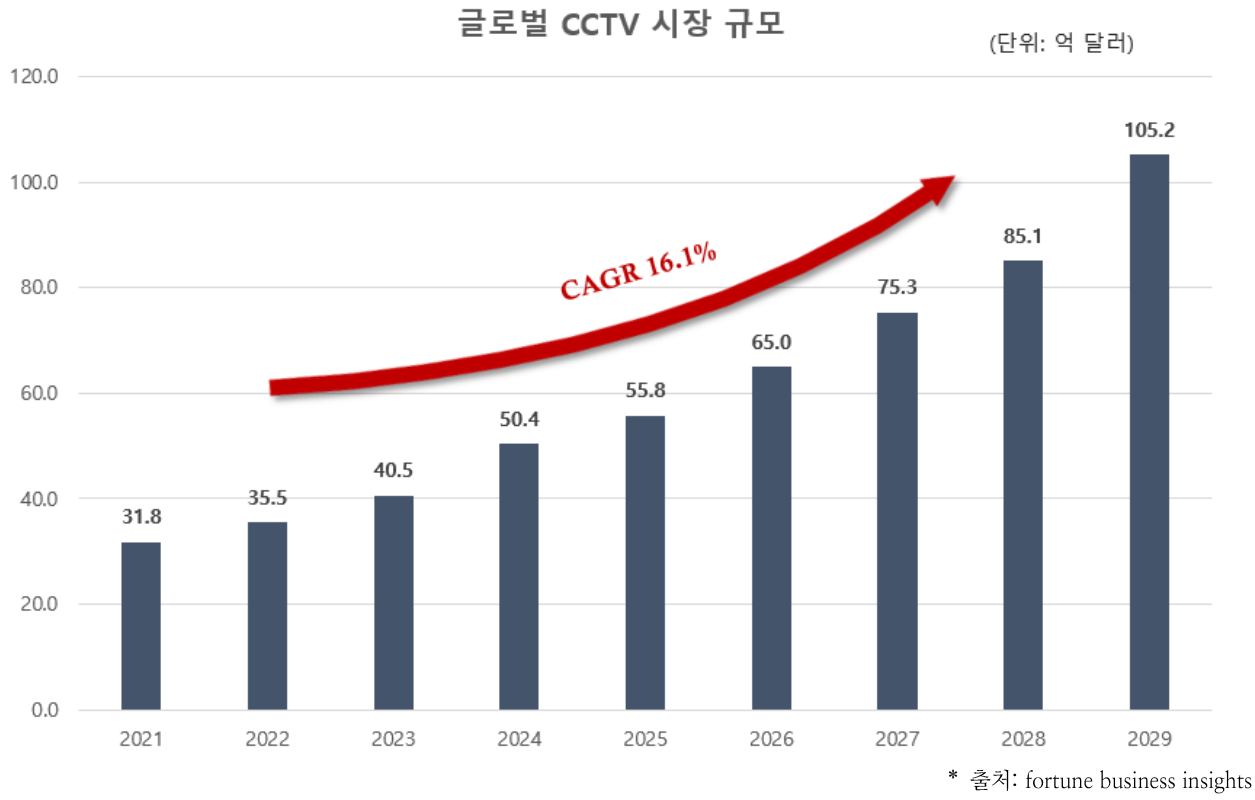
EQST(이큐스트)는 'Experts, Qualified Security Team'
이라는 뜻으로 사이버 위협 분석 및 연구 분야에서 검증된
최고 수준의 보안 전문가 그룹입니다.

infosec

Contents

■ 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.

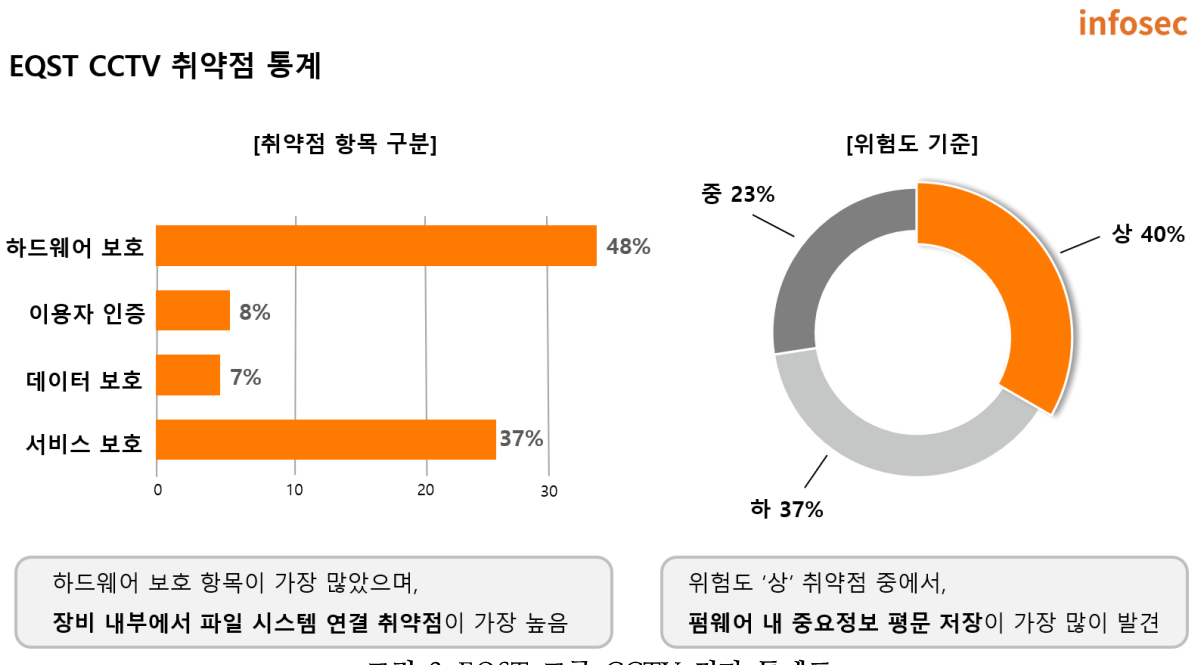


그림 3. EQST 그룹 CCTV 진단 통계표

■ EQST 그룹 CCTV 진단 프로세스

EQST 그룹에서 진행하고 있는 CCTV 디바이스 진단 프로세스는 아래와 같다.

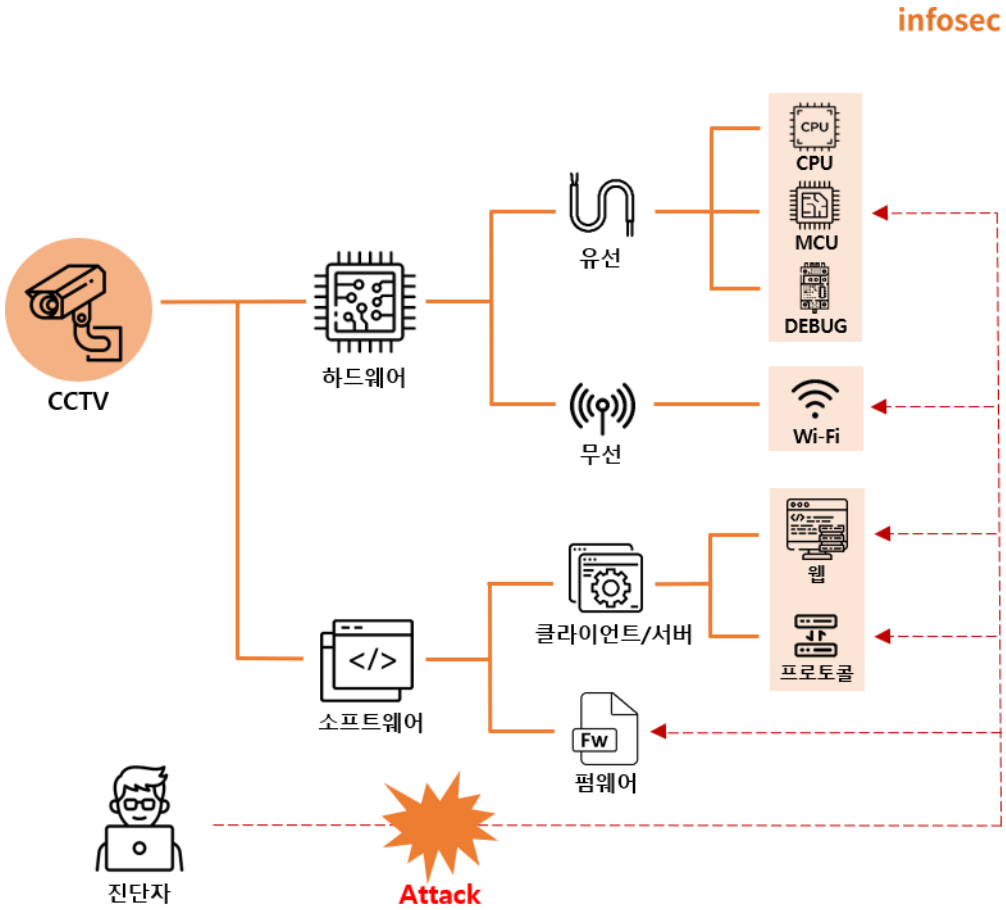


그림 4. EQST 그룹의 CCTV 진단 프로세스 설계도

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.

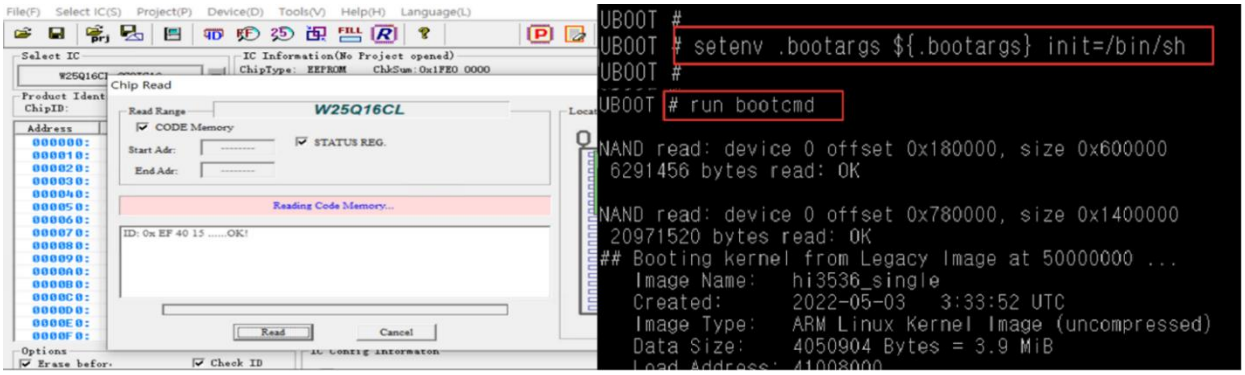


그림 5. MCU 칩을 이용한 펌웨어 추출

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.

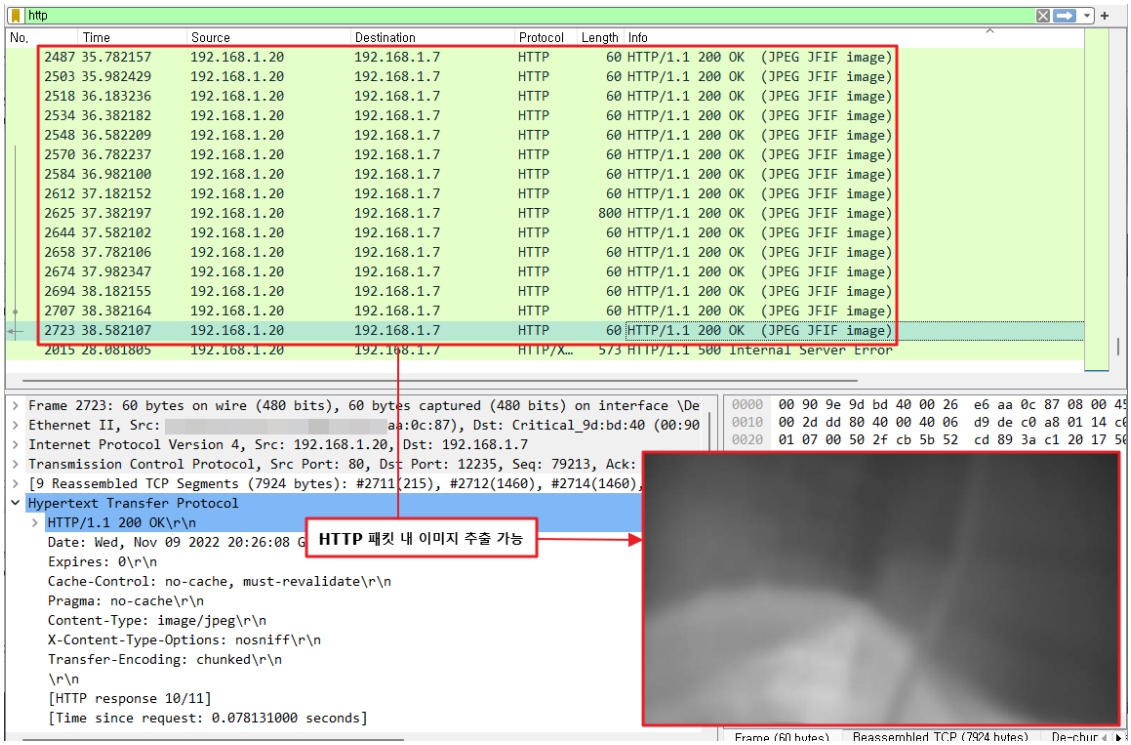


그림 8. HTTP 프로토콜 내 평문 영상정보 노출

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 : RC4 는 1987 년 RSA 시큐리티의 로널드 라이베스트(Ron Rivest)에 의해 개발된 스트림 암호로 1995 년부터 SSL 의 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

Keep up with Ransomware

Clop, 취약점 악용 대규모 공격 위협

■ 개요

2023 년 6 월 랜섬웨어 피해 사례 수는 439 건을 기록했다. 이는 전월(508 건) 대비 69 건 적은 수로 다소 감소세를 보이고 있다. 지난 5 월 랜섬웨어 피해 사례가 많이 나타난 원인은 Malas 가 이메일 플랫폼 Zimbra Collaboration Suite 에 대한 취약점(CVE-2022-24682[11])을 악용하여 171 건의 대규모 공격을 성공시켰기 때문이다.

이번 달에 눈여겨볼 만한 이슈는 Clop 이 또 한 번의 대규모 공격을 수행했다는 것이다. Clop 은 지난 2 월과 4 월에 이어 6 월에도 대규모 공격을 수행한 것으로 확인됐다. Clop 은 Progress MOVEit Transfer 의 취약점(CVE-2023-34362[12])를 악용해 피해자들의 데이터를 다크웹 유출 사이트에 게시하고 금전을 요구했다. 2021 년 7 월에도 CVE-2023-34362 를 악용한 공격 테스트를 진행한 정황이 포착되는 등 Clop 이 이번 공격을 수행하기 위해 오랜 기간 준비한 것으로 보인다. 앞으로도 이번 사건으로 인한 피해자들의 데이터가 유출 사이트에 지속적으로 게시될 가능성이 있어 좀 더 주시할 필요가 있다. 이러한 Clop 의 연이은 대규모 공격으로 인해 미국 정부는 Clop 에 대한 정보를 제공하는 사람에게 1,000 만 달러의 현상금을 제공한다고 밝히며 수사기관의 관심이 Clop 을 향해 집중되고 있다.

또한, LockBit 의 활동은 지난 5 월에 비해 다소 주춤한 양상을 보였으나, 대만 소재 반도체 제조 기업 TSMC(Taiwan Semiconductor Manufacturing Co.)의 민감 데이터를 다크웹에 공개할 것이라고 협박하며, 몸값으로 7,000 만 달러(한화로 약 905 억 원)를 요구했다. 다만, LockBit 이 현재까지 미국 기업을 대상으로만 벌어들인 수익이 9,100 만 달러인 점을 감안했을 때 LockBit 의 협상 요구가 받아들여질지는 의문이다.

[11] CVE-2022-24682 : 피해자 브라우저의 보안 컨텍스트에서 스크립트 코드를 실행할 수 있는 Cross Site Scripting 취약점

[12] CVE-2023-34362 : 웹 쉘 업로드를 가능하게 하는 SQL Injection 취약점

BlackCat(Alphv) 그룹도 꾸준한 행보를 보이고 있다. BlackCat 은 2 월에 미국의 토론 사이트인 Reddit 을 공격했다고 밝혔다. 이후 4 월과 6 월에 Reddit 측에 금전을 요구하는 이메일을 전송했으나, Reddit 이 이에 응답하지 않아 유출 사이트에 80GB 에 상당하는 압축된 주요 기밀 데이터를 유출하겠다는 의사를 표했다. 하지만 Reddit 측은 BlackCat 그룹이 피싱을 통해 한 직원의 자격 증명을 획득하여 일부 내부 문서, 코드, 일부 내부 대시보드 및 비즈니스 시스템에 대한 액세스 권한 정도만 얻었다고 밝히면서 진실공방이 지속되고 있다.

Clop 의 취약점 악용 MOVEit 공격과 BlackCat 의 Reddit 공격 사례의 공통점은 랜섬웨어를 공격에 사용하지 않고 데이터 탈취에 중점을 두었다는 점이다. 이와 비슷한 사례가 이전에도 존재했다. 지난 1 월 BianLian 그룹은 체코의 보안기업 Avast 가 랜섬웨어 복호화 도구를 공개한 후 랜섬웨어를 통한 데이터 암호화 대신에 순수 데이터 탈취로 노선을 전환했다. 이는 랜섬웨어 그룹들이 암호화를 배제한 데이터 탈취를 통해 유출 사이트에 데이터를 게시하여 몸값을 요구하는 형태로도 움직이고 있음을 알 수 있다. 그러나 여전히 랜섬웨어의 실제 사용은 크게 감소하지 않았으며, 사이버 범죄에서 널리 사용되고 있다. 또한 서비스형 랜섬웨어 그룹의 공격 방법이 변화하고 있는 점도 주목할 필요가 있다. 랜섬웨어 그룹들은 IAB[13] (Initial Access Brocker)같은 전문 인력과 협력, 그룹 내에 전문적인 인력 고용 등 조직화된 모습을 보이고 있다.

이 외에도 6 월 다수의 활동을 수행했던 랜섬웨어 그룹으로는 8Base 가 있다. 8Base 의 유출 사이트는 5 월 공개되었으나, 유출 사이트에 2022 년 4 월부터 탈취한 것으로 추정되는 유출 데이터가 게시되었기 때문에 약 1 년간 조용히 활동했을 것이라고 추정된다. 8Base 는 6 월에만 44 건, 총 115 건의 유출 데이터를 게시하고 있다. 또한, 8Base 는 유출 사이트의 유사성과 사실상 동일한 랜섬노트와 서비스 약관으로 인해 RansomHouse 에서 비롯된 그룹이라는 가능성이 제기되고 있다. 다만, 8Base 가 사용하는 SmokeLoader[14]를 통해 로드되는 커스텀 된 Phobos 랜섬웨어는 서비스형 랜섬웨어기 때문에, 해당 랜섬웨어 사용만으로 소속을 나타내는 지표로 보기는 어려운 측면이 존재한다. 따라서 아직 8Base 가 어떤 그룹에서 비롯되었는지 단정 짓기는 어렵다.

6 월에 새로 발견된 랜섬웨어 변종 중 주목할 만한 랜섬웨어는 Royal 랜섬웨어 기반의 Linux 타깃 BlackSuit 이다. BlackSuit 랜섬웨어는 Windows 및 Linux 시스템 모두를 대상으로 하는 범용성을 갖고 있다. 이중 협박 방식을 채택했으며, 파일 암호화에 AES 방식을 적용하였고 암호화 키는 RSA 로 보호했다. 또한, 간헐적 암호화를 통해 암호화 프로세스의 속도를 향상시켰다.

[13] IAB : 초기 침투 경로를 판매하는 개인 혹은 집단

[14] SmokeLoader : 감염된 시스템에 다른 악성코드를 다운로드 하는데 사용하는 악성코드

또한 신규 랜섬웨어 그룹인 Lapiovra 와 NoEscape 가 발견됐다. Lapiovra 그룹은 미국의 나노 기술 연구 기업의 유출 데이터를 게시하며 활동을 시작했다. Lapiovra 그룹이 사용하는 랜섬웨어는 Config 데이터, 사용자의 키보드 언어 식별, C&C URL 생성 루틴 등 REvil(Sodinokibi) 그룹의 랜섬웨어와 유사성이 짙어 이를 기반으로 제작된 것이라고 추측된다. NoEscape 그룹은 이번 달에 발견되었지만 금융, 교육, 제조업 등 다양한 산업 분야에서 7 건의 유출 데이터를 게시하며 활발한 활동을 보이고 있다. NoEscape 랜섬웨어는 서비스형 랜섬웨어로 운영되며 파일에 임의의 문자열을 추가한다는 점 및 랜섬노트가 Avaddon 랜섬웨어와 유사하다. NoEscape 는 Windows 타깃의 랜섬웨어뿐만 아니라 Linux, ESXi 시스템을 타깃으로 하는 변종 또한 보유하고 있는데, 특히 Windows 타깃 랜섬웨어에서는 Reflective DLL Injection[15] 기법을 사용한다는 특징을 가지고 있다.

한편 국내에서는 여전히 취약하게 관리되고 있는 MS-SQL 서버를 대상으로 하는 Mallox 랜섬웨어가 유포되고 있다. 특이한 점은 EXE 파일뿐 아니라 BAT 파일 확장자도 사용되고 있다는 것이다. BAT 파일은 Windows 에서 사용되는 스크립트 파일로 일련의 작업을 자동화할 때 주로 사용한다. 이를 통해 파워쉘 스크립트를 실행하여 악성코드 페이로드 전달이 가능하므로, 공격자 입장에서 탐지 우회를 위해 사용한다. 이를 이용해 Mallox 랜섬웨어는 취약한 시스템에서 관리하고 있는 자격 증명에 대해 Brute Force Attack[16]이나 Dictionary Attack[17]을 수행하여 초기 침투를 수행하고 있다.

또한, Crysis 랜섬웨어를 사용하는 그룹이 취약한 RDP 를 통해 역시 Brute Force Attack 이나 Dictionary Attack 로 계정 정보를 획득하여 Venus 랜섬웨어를 유포한 정황이 확인됐다. 이들은 Venus 랜섬웨어를 포함하여 포트 스캐너, Mimikatz 와 같은 도구를 설치하여 네트워크 확산을 발생시켰다. 따라서 Crysis 랜섬웨어로 인해 피해를 입었을 경우 내부 시스템에 전파된 정황을 확인할 필요가 있으며, 올바른 패스워드 정책을 따르고 시스템을 최신 버전으로 유지하는 것이 중요하다.

[15] Reflective DLL Injection : 실행중인 프로세스의 메모리에 DLL 의 데이터를 삽입한 후 직접 매핑하여 실행시키는 기법

[16] Brute Force Attack : 암호를 풀기 위해 가능한 모든 값을 대입하는 기법

[17] Dictionary Attack : 사전에 있는 단어를 입력하여 암호를 알아내는 기법

■ 랜섬웨어 뉴스

infosec

Clop, MOVEit Transfer 제로데이를 대규모 데이터 탈취에 악용

- Clop 그룹, MOVEit Transfer의 취약점 CVE-2023-34362 악용
- 취약점을 악용해 웹 쉘을 배포하여 지속성 유지 및 인증 수행
- 1400개 이상의 호스트가 위험에 노출
- 암호화를 수행하지 않고 몸값 요구

Clop, MOVEit Transfer 취약점을 2021년부터 테스트한 정황 확인

- 피해 시스템에서 로그 분석 중 2021년부터 테스트한 정황 확인
- 2021년 7월에도 유사한 활동 증거 확인
- 수백 개 회사가 피해를 입은 것으로 추정

Akira 랜섬웨어, 무료 복호화 도구 개발

- Avast 社, 무료 Akira 복호화 도구 개발 및 배포
- Windows 기반의 32비트 및 64비트 복호화 도구 개발

BlackCat(Alphv), Reddit 데이터 유출 위협

- BlackCat, Reddit에서 탈취한 80GB 상당의 압축 데이터 공개 협박
- 2월에 수행한 피싱 공격으로부터 비롯됨

Rhysida, 칠레 군대에서 탈취한 문서 유출

- 한 육군 상병이 해당 공격에 연루됨
- 약 360,000개의 칠레 육군 관련 문서 게시, 자신들이 탈취한 데이터 중 30%만 공개했다고 주장
- Cobaltstrike 등을 사용하여 네트워크 확산 후 랜섬웨어 페이로드 드랍

* CobaltStrike : 상용 침투 테스트 도구, 크랙 버전이 공개되어 악용됨

미국에서 LockBit 계열사로 의심되는 용의자 기소

- 작년 11월 이후로 미국에서 세 번째로 LockBit 계열사 기소
- 최소 5건 이상의 공격을 직접 수행

미국 정부, Clop 랜섬웨어 정보 제공에 1,000만 달러 현상금 제공

- 미 국무부, Clop 랜섬웨어 그룹 정보 제공자에게 현상금 제공하기로 발표
- Clop을 비롯한 공격자에 대한 정보를 제출하기 위한 서버 구축

LockBit, TSMC 협력사 공격 후 7천만 달러(약 905억 원) 요구

- LockBit 그룹, TSMC 협력사 '킨맥스(Kinmax)'의 내부 프로그램에 접근하여 데이터 탈취 후 7천만 달러의 금액을 요구
- TSMC 측은 본사와 고객에 영향을 미치지는 않았으나 해당 협력사와는 협력을 중단하였다고 발표

WannaCry 랜섬웨어를 사칭하여 러시아 게임 유저 공격

- WannaCry 랜섬웨어를 사칭하여 러시아의 FPS 게임 유저들을 공격
- 무료로 공개된 게임이므로 설치 프로그램 다운로드 후 악성 페이로드 삽입 후 배포 가능
- WannaCry를 사칭했으나, 교육용으로 만들어진 오픈 소스 'Cypter' 암호화 도구 악용하여 제작
- 피해자를 위협하고 몸값 지불의 부담을 가중시키기 위해 WannaCry 모방

랜섬웨어 공격자, 암호화폐 세탁을 위해 클라우드 마이닝 서비스 활용

- 북한에 기반을 둔 APT43이 클라우드 마이닝 서비스를 사용하여 안티 포렌식 수행 후 암호화폐 세탁
- 클라우드 마이닝은 원격으로 코인을 채굴할 수 있는 서비스
- 자금 출처를 모호하게 만들고 자금의 원천이 합법적인 수단처럼 보이게 만듦

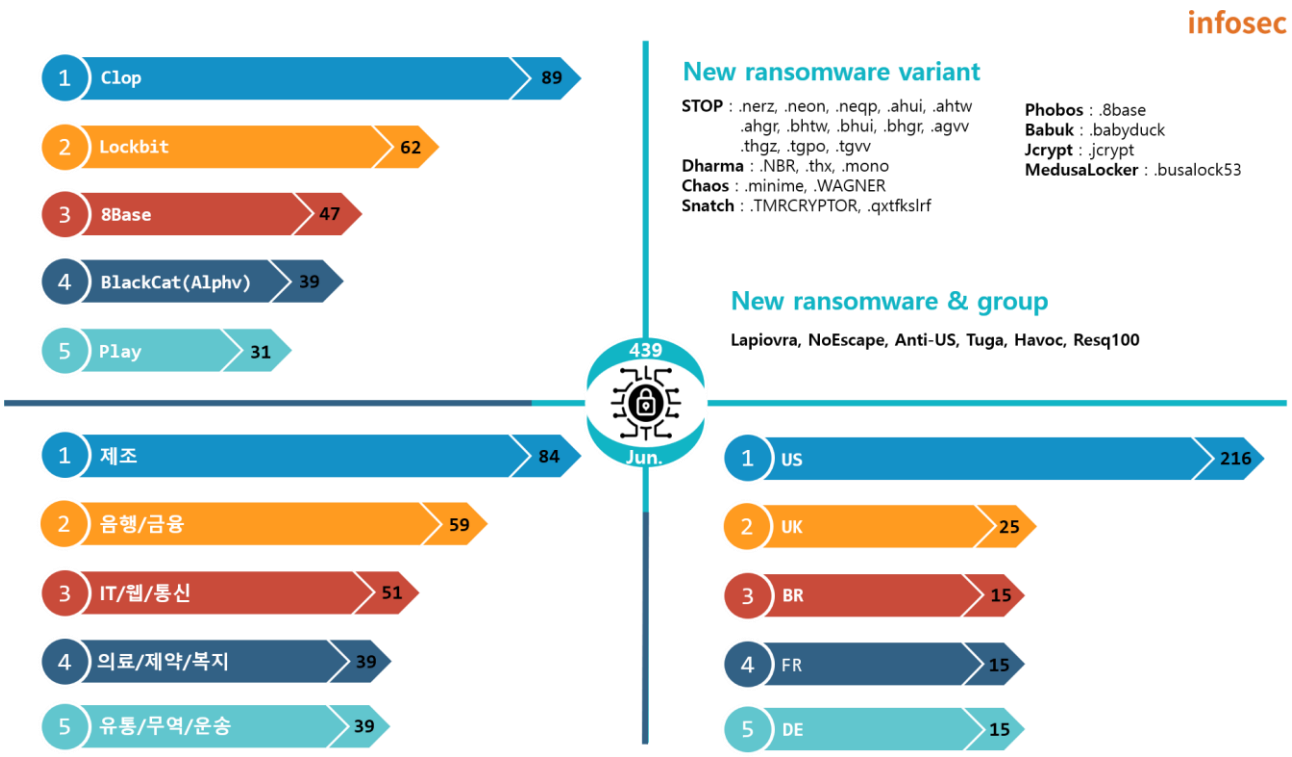
Cyclops 랜섬웨어 그룹, 포럼에서 Go 기반의 정보 탈취형 악성코드 판매

- Cyclops, 감염된 시스템에서 중요한 데이터를 캡처하도록 설계된 정보 탈취형 악성코드 판매
- Windows 및 Linux를 타깃으로 설계되어 원하는 데이터 탈취 가능

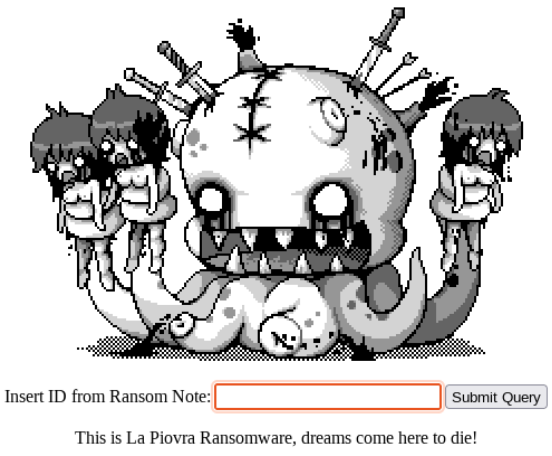
TargetCompany 랜섬웨어 그룹, Mallox 변종 Xollam으로 활동

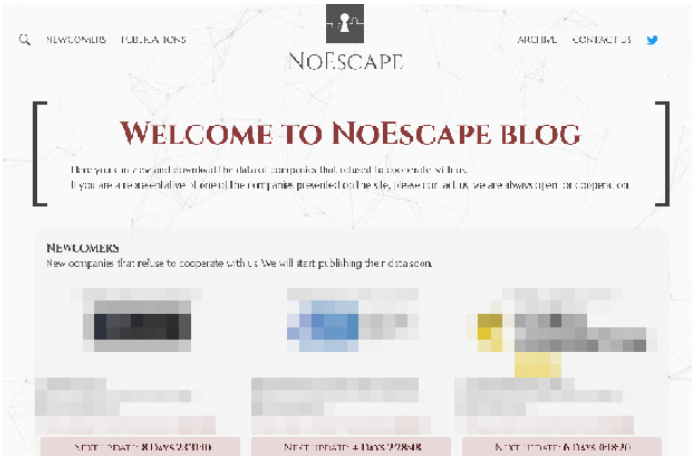
- Xollam, 악성 Ms OneNote 파일을 첨부파일로 한 스팸 메일을 통해 확산
- TargetCompany 랜섬웨어 그룹, 이중 협박을 위해 텔레그램 채널을 개설

■ 랜섬웨어 위협



새로운 위협





*출처: Lapiovra, NoEscape 랜섬웨어 그룹 사이트 이미지

2023 년 6 월 랜섬웨어 피해 사례는 439 건으로 지난 5 월 508 건에 비해 비교적 적은 수를 기록했지만 신종 및 변종 랜섬웨어가 꾸준히 등장하고 있어 여전히 위험한 상황이다. 게다가 과거 랜섬웨어 그룹들은 랜섬웨어 공격을 위한 초기 침투 과정에 많은 시간과 자원을 투자해왔지만, 오늘날에는 랜섬웨어 생태계가 조직화되면서 이러한 판도가 변화하기 시작한 점이 차별점이다.

특히, 최근에 등장한 서비스형 랜섬웨어 그룹은 계열사나 공격자를 모집하여 권한을 위임하고, 이들은 IAB 에게 일정 금액을 지불하여 초기 침투 경로를 얻어 피해자의 네트워크에 침투한다. 그 후 파일을 탈취하고 암호화하여 파일 복호화와 데이터 유출을 빌미로 이중 협박을 하고 금전을 갈취한다. 이들이 계열사를 통해 공격을 수행했을 경우에는 계열사에서 일정 금액을 수거해 총책에게 일정 비율을 분배하며, 공격자가 공격을 수행한 경우 총책이 금액을 수거해 일정 비율로 공격자에게 분배한 뒤 믹싱 서비스를 통해 자금을 세탁한다. 이러한 IAB 시장의 활성화로 인해 랜섬웨어 그룹들은 초기 침투를 쉽고 빠르게 성공시킬 수 있을 뿐만 아니라 이를 통해 단시간에 대량의 공격을 수행할 수 있어 위험성이 커지고 있다.

6 월에 발견된 주목할 만한 변종 랜섬웨어는 Linux 기반의 BlackSuit 랜섬웨어다. 이 랜섬웨어는 Royal 랜섬웨어 그룹이 운용하는 랜섬웨어로 Windows 와 Linux 모두를 타깃으로 하는 랜섬웨어로 알려져 있다. 또한 배포를 위해 IcedID[18] 와 Emotet[19] 을 로더로 사용하는 방식을 개발 중이다. BlackSuit 랜섬웨어는 바이너리 파일 비교 도구를 통해 확인한 결과 약 98% 이상의 유사도를 보일 정도로 Royal 랜섬웨어 그룹과 유사성이 굉장히 높다. BlackSuit 은 아직 Royal 랜섬웨어만큼 활성화되지 않았으나, 지속적인 테스트를 거치고 있어 추후 BlackSuit 로 리브랜딩이 이루어질지, 특정 조건에 부합하는 대상에게만 사용할지는 조금 더 지켜봐야 알 수 있을 것으로 추측된다.

이번 달에 발견된 신규 랜섬웨어 그룹은 Lapiovra, NoEscape 가 있다. 특히, Lapiovra 는 REvil(Sodinokibi) 코드와 상당한 유사점을 보인다. 특히, C&C URL 생성 루틴과 특정 언어를 사용하는 사용자의 암호화를 피하고 Config 데이터 역시 구조가 유사한 점이 확인됐다. 이를 통해 REvil(Sodinokibi) 랜섬웨어의 코드를 구입하거나 제공받아 제작한 랜섬웨어라고 추측된다.

NoEscape 그룹은 지속적으로 서비스형 랜섬웨어를 통해 계열사 모집을 홍보하고 있다. 타 그룹의 코드를 사용하지 않고 C++ 언어로 자체 개발한 랜섬웨어를 사용하고 있으며, ChaCha20 과 RSA 알고리즘을 혼합한 하이브리드 암호화 방식을 채택했다. 더불어, Windows 와 Linux 및 VMWare ESXi 공격을 모두 지원한다는 특징을 가지고 있다. 또한 계열사가 추가금을 지불하면 DDoS 를 수행할 수 있는 서비스도 제공하는데, 이는 기존 이중 협박에 더해 DDoS 공격을 통한 추가 협박을 진행하여 피해자에게 몸값 지불의 부담을 가중시킬 가능성이 높다. 한편 이들은 CIS 국가[20] 의 법인을 대상으로는 공격을 수행하지 않도록 조건을 두고 있어, 공격자가 CIS 국가와 관련이 있을 수도 있다고 추측할 수 있다.

---

[18] IcedID : 주로 기업을 대상으로 결제 정보를 훔치는 역할을 하며 다른 악성코드를 전달하거나 추가 모듈을 다운로드 하는 악성코드

[19] Emotet : 다른 악성코드를 다운로드하고 설치하는 데 사용되는 트로이 목마

[20] CIS 국가 : 소련의 해체로 독립한 국가들의 국제기구. 러시아, 몰도바, 벨라루스, 우즈베키스탄, 카자흐스탄 등이 포함됨

Top5 랜섬웨어

6 월에도 제조업을 중심으로 많은 랜섬웨어 공격이 집중됐다. 국가 별로 이루어진 공격을 살펴보면, Top5 랜섬웨어 모두 미국을 대상으로 한 공격을 가장 많이 수행한 것으로 확인할 수 있다. 피해 사례 수의 경우, 지난달에 비해 소폭 감소하였지만 Clop 은 MOVEit Transfer 취약점을 악용한 대규모 공격을 수행했고, 피해자의 데이터를 지속적으로 게시하고 있는 상태다.

LockBit 은 지금까지 미국의 기업들로부터 총 9,100 만여 달러를 갈취하는 등 상당한 영향력을 과시하고 있는 랜섬웨어 그룹이다. 최근 미국과 러시아에서 LockBit 그룹의 공격에 가담한 이들에 대한 체포 소식이 나오는 것을 봤을 때 수사기관의 이목이 집중되었다는 것을 알 수 있다. 이러한 수사기관의 압박으로 인해 Clop 의 공격 규모가 줄어든 것으로 추측되며, Clop 의 대규모 공격 이슈로 이목이 집중되어 유출한 데이터 공개를 미루는 등 다양한 원인으로 주춤하는 모습을 보이고 있다.

그럼에도 불구하고 LockBit 은 여전히 많은 수의 피해자를 발생시키고 있다. 6 월 말경, LockBit 은 대만 소재 반도체 제조 기업인 TSMC 의 민감 데이터를 다크웹에 공개하겠고 협박하며 몸값으로 7,000 만 달러(한화로 약 905 억 원)를 요구했다. 그러나 Kinmax 측은 확인 결과 네트워크의 특정 환경이 취약했음을 알게 되었고, 유출된 내용은 회사가 고객에게 기본 구성으로 제공한 시스템 설치 내용이 주를 이뤘다고 밝혔다. 또한 TSMC 는 비즈니스 운영에 영향이 없고 고객 정보 역시 안전하다고 밝혔다. 아직 협상 결과는 공개되지 않았으나 만약 LockBit 그룹의 주장이 사실이라면 상당한 규모의 피해가 발생할 것으로 예상된다.

이번 달에 새롭게 Top5 랜섬웨어에 등장한 8Base 는 1 년 동안 피해자를 공개하지 않고 조용히 활동한 정황이 포착되어 앞으로 어떤 활동을 이어 나갈지 눈여겨볼 필요가 있다. 8Base 의 랜섬노트는 유출된 Babuk 의 ESXi 타깃 변종 랜섬노트와 많은 유사점을 공유하고 있으며 그 내용은 다른 랜섬노트에 비해 상세한 편이다. 내용을 보면, 특히 제 3 자의 개입을 금지하는 내용이 담겨있으며 탈취한 데이터를 외부에 공개하지 않겠다는 보증이 작성되어 있고, 오로지 비트코인으로만 몸값을 지불 받는다고 기재되어 있다.

BlackCat(Alphv)은 6 월 17 일에 다크웹 유출 사이트에 Reddit 에 대한 글을 게시했다. 해당 글에서 지난 2 월에 Reddit 을 공격하여 데이터를 탈취하였다고 주장하며 Reddit 측이 협상에 응하지 않아 데이터를 유출할 예정이라는 계획을 밝혔다. BlackCat 측은 주요 기밀 데이터가 담긴 상당한 양의 압축 파일을 보유하고 있다고 주장하고 있으며, Reddit 측은 일부 데이터와 액세스 권한만을 침해당했다고 주장하고 있어 아직 어떤 상황인지 파악하기에는 조심스러운 상황이다. Play 랜섬웨어 그룹도 이번 달에만 건설, 제조, IT 분야 등 총 27 건의 피해자의 데이터를 유출 사이트에 게시하며 활발한 활동을 이어가고 있다.

■ 랜섬웨어 집중 포커스

Clop 의 MOVEit Transfer

Clop 랜섬웨어는 TA505 로 식별되는 그룹이 운용하고 있는 랜섬웨어로, 2016 년 3 월 발견된 CryptoMix 랜섬웨어에서 진화된 랜섬웨어다. 이 그룹은 꾸준히 취약점을 통한 대규모 공격을 일삼고 있는데, 지난 2 월에 파일 전송 솔루션인 GoAnywhere MFT 의 취약점(CVE-2023-0669 [21])을 악용하여 공격을 수행한 것을 시작으로 4 월에는 프린터 솔루션인 PaperCut 의 취약점(CVE-2023-27350 [22])을 통한 공격을 수행, 6 월에는 파일 전송 솔루션인 Progress 의 MOVEit Transfer 의 취약점을 악용하여 수행한 공격의 피해 사례를 유출 사이트에 점차적으로 게시하고 있는 상황이다.

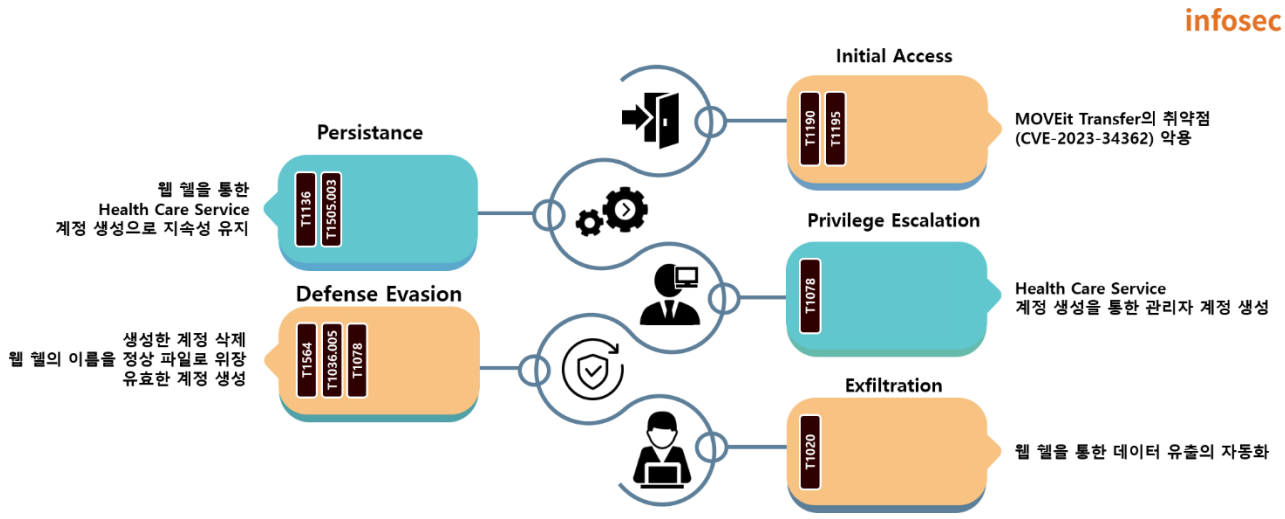
이번 MOVEit Transfer 공격에서의 특이점은 랜섬웨어를 이용한 암호화 전략을 사용하지 않았다는 것이다. 데이터를 암호화하는 대신에 탈취하는 전략을 선택한 Clop 은 Bleeping Computer 와의 인터뷰에서 데이터 암호화 대신 데이터 탈취를 더 선호한다고 밝히기도 하였다.

---

[21] CVE-2023-0669 : GoAnywhere MFT 에서 발생할 수 있는 원격 코드 실행 취약점

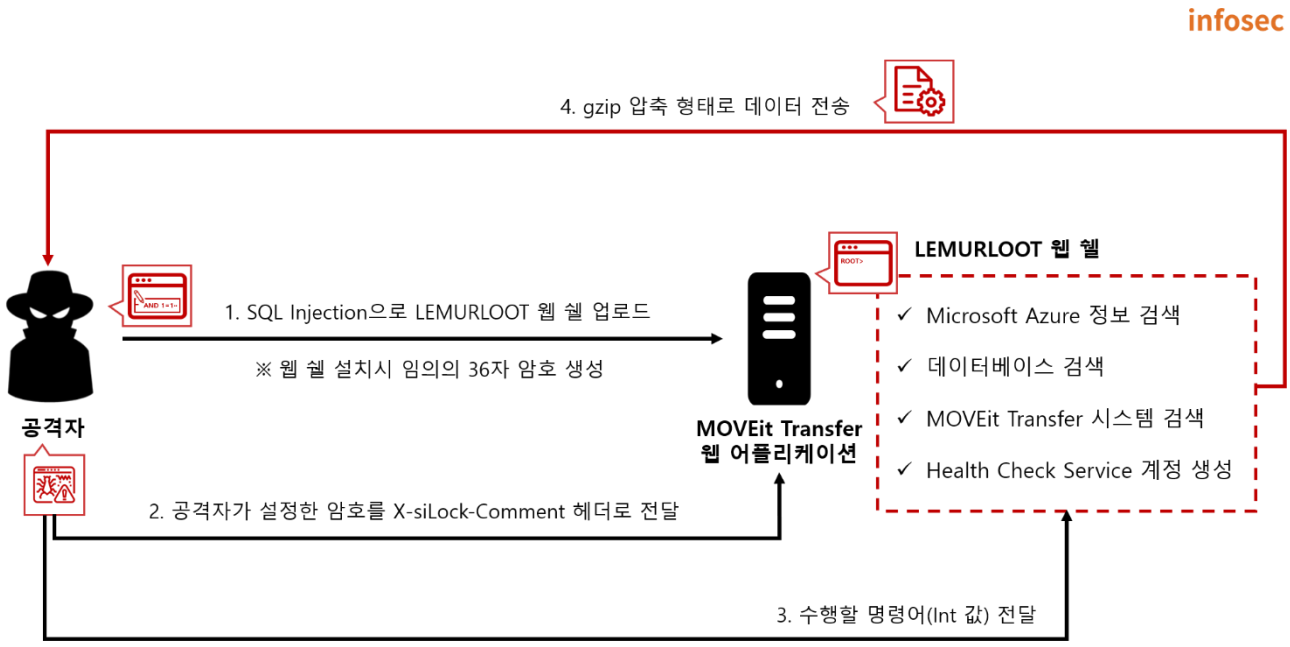
[22] CVE-2023-27350 : PaperCut 에서 발생할 수 있는 원격 코드 실행 취약점

Clop 의 MOVEit Transfer 공격 전략



Clop 은 MOVEit Transfer 의 취약점(CVE-2023-34362)을 악용하여 웹 쉘을 업로드하여 공급망 공격을 수행했다. 이때 사용된 웹 쉘은 MOVEit Transfer 의 구성요소인 human.aspx 를 가장한 human2.aspx 라는 이름으로 업로드됐다. 이 웹 쉘은 지속성을 유지하며 Health Care Service 라는 계정 생성을 통해 관리자 계정을 생성하여 권한 상승 후 특정 데이터 및 Azure 에 저장된 파일을 탈취했다. 거기에 추후 침해 사고 분석을 방해하기 위해 생성한 계정을 삭제하는 치밀함을 보였다.

Clop 의 MOVEit Transfer 공격 시나리오



Clop 은 MOVEit Transfer 공격에서 백도어 역할을 하는 LEMURLOOT 라는 웹 쉘을 서버에 SQL Injection[23] 공격을 통해 설치했다. 해당 웹 쉘은 MOVEit Transfer 사용자가 업로드한 데이터와 Azure Storage Blob[24] 정보를 포함한 자격 증명을 탈취하는 기능을 수행한다. 백도어에 대한 명령은 HTTP 요청으로 전달이 되는데, X-siLock-Comment 헤더를 통해 공격자가 인증을 수행한다.

공격이 성공하기 위해서는 X-siLock-Comment 헤더에 공격자가 지정한 특정 비밀번호를 함께 전송하여 웹 쉘에 인증을 수행해야 한다. 비밀번호 인증 후 명령어 값을 전달하면 웹쉘은 다음과 같은 동작을 수행한다.

① Microsoft Azure 시스템 설정, Azure Blob Storage, Azure Blob Storage 계정, Azure Blob 키 및 Azure Blob Container를 검색하고 DB 내의 필드를 열거한다.
② 공격자가 전송한 문자열과 일치하는 문자열을 이름으로 갖는 파일을 MOVEit Transfer 시스템에서 검색한다.
③ 임의로 생성된 사용자 이름과 "Health Care Service"로 설정된 LoginName 및 Real Name 값을 사용하여 새 관리자 권한 계정을 만든다.
④ LoginName 및 RealName 값이 "Health Care Service"로 설정된 계정을 삭제한다.

[23] SQL Injection : 공격자가 악의적인 SQL 코드를 입력하여 데이터베이스에 비인가된 액세스를 획득하는 공격

[24] Azure Storage Blob : Azure 클라우드 환경에서 대용량 데이터를 저장하고 관리하기 위한 플랫폼

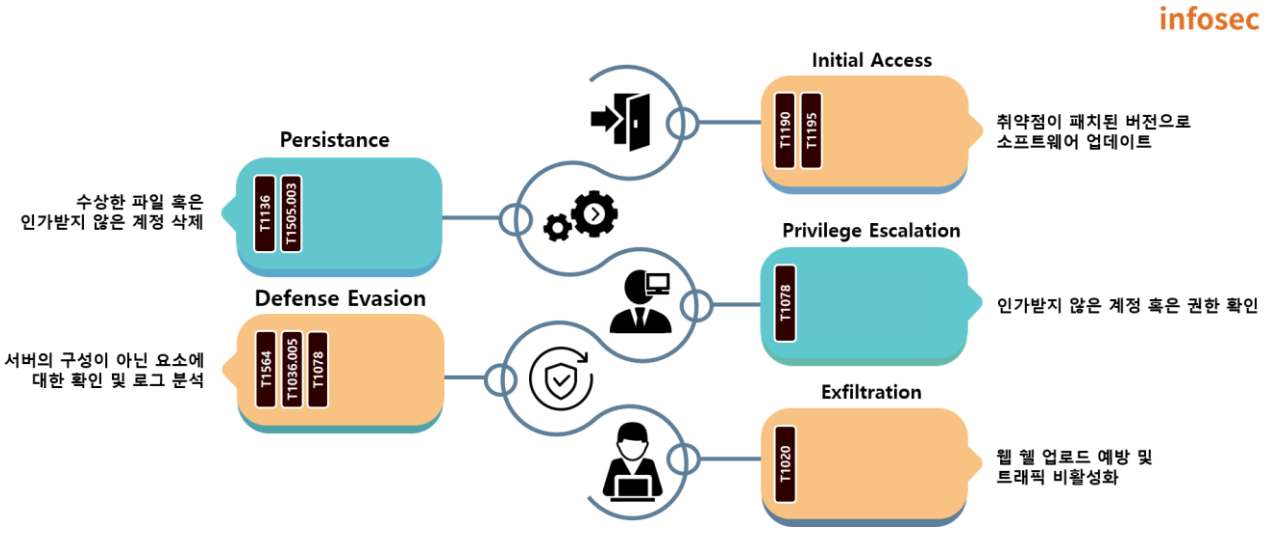
Clop 은 이러한 명령을 수행하는 웹 쉘을 통해서 원하는 파일을 탈취할 뿐 아니라 언제든 다시 시스템에 접근하기 위해서 Health Care Service 라는 계정을 생성하여 지속성을 유지했다. 심지어 Azure 클라우드에 저장한 데이터에까지 접근하기 위해 Azure Storage Blob 의 정보를 탈취하는 치밀함을 보였다. 이렇게 탈취한 데이터를 gizp 형태로 압축하여 공격자는 다운로드를 통해 손에 넣게 된다.

만약 X-siLock-Comment 헤더와 함께 전송된 암호가 유효하지 않을 경우에는 백도어가 존재하지 않는 것처럼 위장하기 위해 404 상태 코드[25]로 응답한다. 그 후, 데이터 베이스와의 연결을 종료하고 웹 쉘이 종료된다. 이때 암호는 웹 쉘 파일마다 다르기 때문에 다양한 IoC[26](Indicator of Compromise)가 존재하게 된다.

[25] 404 상태 코드 : 웹 서버가 클라이언트의 요청에 대해 해당 리소스를 찾을 수 없다는 것을 나타내는 오류 코드

[26] IoC : 컴퓨터 시스템 혹은 네트워크에서 침해 사고를 분석하는데 사용하는 지표. 해시, IP, 파일명 등이 포함됨

Clop 의 MOVEit Transfer 공격 단계별 대응 방안



MOVEit Transfer 취약점을 통한 초기 침투를 막기 위해서는 취약점이 패치된 버전의 소프트웨어를 설치하거나 업데이트하는 것이 효과적이다. 그러나, 즉각적인 조치가 어려운 상황에서는 MOVEit Transfer 환경에 대한 HTTP 트래픽을 비활성화하거나, 서버의 구성요소에 포함되지 않는 수상한 파일이나 인가받지 않은 계정을 삭제하는 작업이 필요하다. 더불어 활성화된 세션을 제거하거나 로그를 검토하는 방안도 침해사고를 예방하는 데 도움이 된다. 거듭 강조하지만 취약점이 패치된 버전의 소프트웨어 사용이 가장 중요하다. 사용하는 소프트웨어 버전을 확인하고 패치가 적용되지 않았다면 신뢰할 수 있는 공식 홈페이지에서 신규 버전을 설치하는 것을 권장한다.

취약한 버전	패치된 버전
MOVEit Transfer 2023.0.0(15.0)	MOVEit Transfer 2023.0.2(15.0.2)
MOVEit Transfer 2022.1.x(14.1)	MOVEit Transfer 2022.1.6(14.1.6)
MOVEit Transfer 2022.0x(14.0)	MOVEit Transfer 2022.0.5(14.0.5)
MOVEit Transfer 2021.1.x(13.1)	MOVEit Transfer 2021.1.5(13.1.5)
MOVEit Transfer 2021.0.x(13.0)	MOVEit Transfer 2021.0.7(13.0.7)
MOVEit Transfer 2020.1.x(12.1)	특수 패치 사용 가능
MOVEit Transfer 2020.0.x(12.0) 이상	지원되는 버전으로 업그레이드 요망

Indicator Of Compromise

human2.aspx : SHA256

0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e90ea05169d11141
5903a1098110c34cdbbd390c23016cd4e179dd9ef507104495110e301d3b5019177728010202c8
096824829c0b11bb0dc0bff55547ead182861826268249e1ea58275328102a5a8d158d36b4fd31
2009e4a2526f0bfbc30de22413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f
31acbc52ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59348e4351
96dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d387cee566aedbafa8c114e
d1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a38e69f4a6d2e81f28ed2dc6df0daf31e73ea
365bd2cfc90ebc31441404cca2643a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d
3c2a74545725b

File Name

human2.aspx : An malicious web shell disguised as human.aspx, which is one of the components of MOVEit Transfer

■ 참고 사이트

URL: https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/

URL: https://thehackernews.com/2023/06/new-linux-ransomware-strain-blacksuit.html

URL: https://www.bleepingcomputer.com/news/security/microsoft-links-clop-ransomware-gang-to-moveit-data-theft-attacks/

URL: https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/

URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

URL: https://thehackernews.com/2023/06/clop-ransomware-gang-likely-exploiting.html

URL: https://www.bleepingcomputer.com/news/security/royal-ransomware-gang-adds-blacksuit-encryptor-to-their-arsenal/

URL: https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-exploiting-moveit-zero-day-since-2021/

URL: https://www.malwarebytes.com/blog/news/2023/06/more-moveit-vulnerabilities-found-while-the-first-one-still-resonates

URL: https://www.securityweek.com/new-moveit-vulnerabilities-found-as-more-zero-day-attack-victims-come-forward/

URL: https://www.bleepingcomputer.com/news/security/cisa-lockbit-ransomware-extorted-91-million-in-1-700-us-attacks/

URL: https://www.bleepingcomputer.com/news/security/suspected-lockbit-ransomware-affiliate-arrested-charged-in-us/

URL: https://www.malwarebytes.com/blog/news/2023/06/moveit-discloses-yet-another-vulnerability-three-times-a-charm

URL: https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response

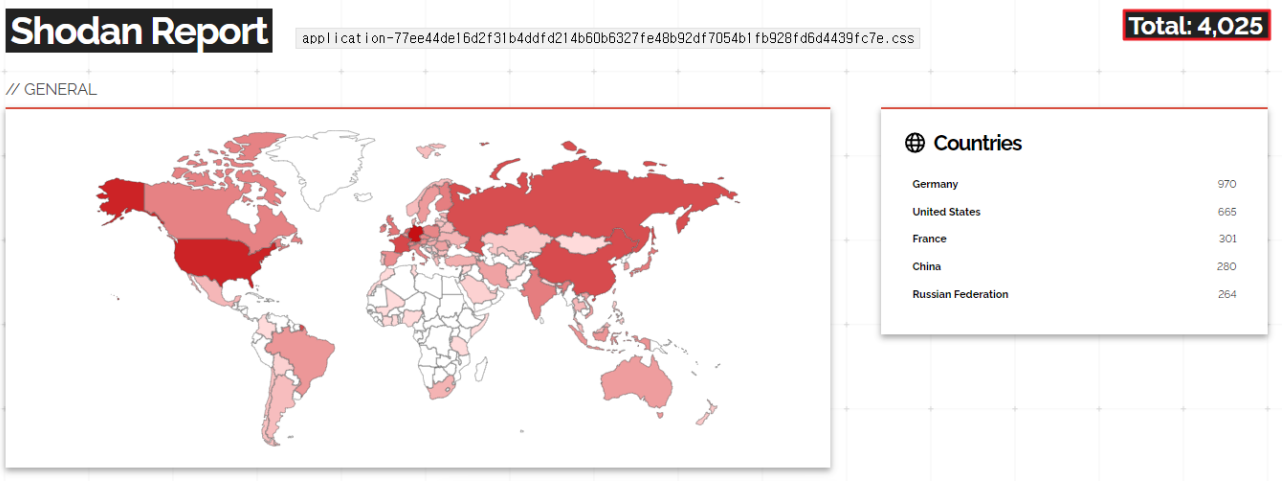
Research & Technique

GitLab 임의 파일 읽기 취약점 (CVE-2023-2825)

■ 취약점 개요

2023 년 5 월, 개인 또는 조직이 소프트웨어 개발 및 협업을 위해 사용하는 Git 리포지토리 관리 솔루션 GitLab 에서 임의 파일 읽기 취약점이 발견됐다. 해당 취약점은 경로 탐색 취약점을 활용해 서버의 임의의 파일을 읽거나 다운받을 수 있기 때문에 GitLab 에서는 CVSS[27] 기준 10.0 점으로 평가했다. 특히, 인증되지 않은 공격자가 공개 프로젝트의 첨부파일 다운로드 경로를 조작해 잠재적으로 서버 주요 데이터 파일인 구성 세부 정보, 기업의 소스 코드, 민감한 사용자 데이터 등에 접근할 수 있어 주의가 필요하다.

인터넷상에서 공개된 취약한 GitLab 은 Shodan 등의 OSINT 검색 엔진을 통해 확인할 수 있다. 지난 6 월 28 일 Shodan 을 이용해 취약한 서버를 검색한 결과, 약 4,000 개의 취약한 GitLab 이 존재하는 것으로 나타났다. 따라서 취약한 버전을 사용한다면 각별한 주의가 필요하다.



*출처: Shodan Report

그림 1. 취약한 서버 검색 결과

[27] CVSS(Common Vulnerability Scoring System)란 컴퓨터 시스템 보안 취약점의 심각도를 평가하기 위한 무료 공개 산업 표준이다.

■ 영향받는 소프트웨어 버전

CVE-2023-2825 에 취약한 GitLab 의 버전은 다음과 같다.

S/W 구분	취약 버전
GitLab CE(Community Edition)/EE(Enterprise Edition)	16.0.0

※ 취약점이 동작하기 위해서는 최소 5 개의 그룹이 존재해야 한다는 조건이 존재한다. 조건은 아래의 취약점 상세 분석을 통해 확인할 수 있다.

■ 공격 시나리오

CVE-2023-2825 취약점을 이용한 공격 시나리오는 다음과 같다.

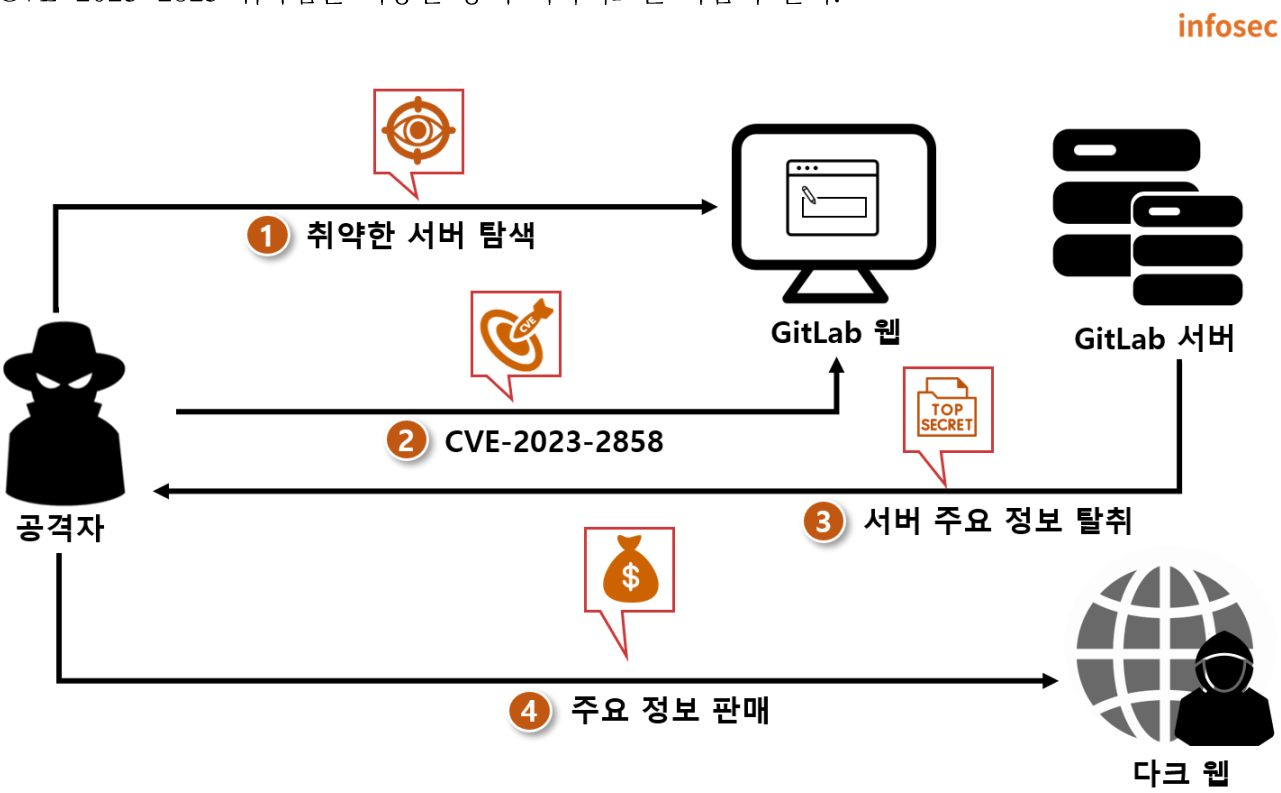


그림 2. 공격 시나리오

① 공격자는 OSINT 검색 엔진을 통해 취약한 GitLab 웹 서버를 탐색
② 공격자는 CVE-2023-2825 취약점을 이용해 피해자 서버에 접근
③ 공격자의 요청을 받은 서버는 주요 정보(개발 소스 코드, 서버 환경 구성 정보 등)를 공격자에게 반환
④ 공격자는 획득한 주요 정보를 다크 웹이나 다른 경쟁사에게 판매

■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2023-2825 의 동작 과정을 살펴본다.

이름	정보
피해자	Ubuntu 20.04.5 LTS (192.168.100.162) GitLab 16.0.0
공격자	Kali Linux 6.1.0-kali5-amd64 (192.168.100.152)

■ 취약점 테스트

Step 1. 환경 구성

1) 피해자 PC 에 docker hub 에서 지원하는 GitLab CE 이미지 중, 취약점이 존재하는 GitLab 16.0.0 버전의 서버를 구축한다.

명령어	$ docker run -d -p 80:80 gitlab/gitlab-ce:16.0.0-ce.0 -d 옵션: detach 모드로 백그라운드로 docker 를 실행시키는 옵션 -p 옵션: local 포트와 docker 에서 실행할 포트를 지정하는 옵션

```
root@ubuntu:/home/eqst# docker run -d -p 80:80 gitlab/gitlab-ce:16.0.0-ce.0
Unable to find image 'gitlab/gitlab-ce:16.0.0-ce.0' locally
16.0.0-ce.0: Pulling from gitlab/gitlab-ce
1bc677758ad7: Pull complete
633fcf47bc79: Pull complete
472c1ac0c258: Pull complete
5b665b492973: Pull complete
0bd8b5a23fe7: Pull complete
b385dd2cb2ca: Pull complete
38ac4d68d24c: Pull complete
e4588a97b783: Pull complete
Digest: sha256:ab90cdb096c4f81247088357b0e051f5b8a999284b2186cbd1b1ec1a41cca7e8
Status: Downloaded newer image for gitlab/gitlab-ce:16.0.0-ce.0
3e524103ef6858b7825c530db4ce0d2dd3c1eb5f1e36776ef413574655d61784
```

그림 3. docker 를 통한 환경 구축

2) GitLab 루트 계정의 패스워드를 재설정하기 위해 컨테이너의 터미널을 열고 아래의 명령어를 실행한다.

명령어	컨테이너 접근 명령어 : $ docker exec -it [container 명 또는 container ID] /bin/bash 패스워드 변경 명령어 : # gitlab-rake "gitlab:password:reset[root]"

```
root@ubuntu:/home/eqst# docker ps
CONTAINER ID   IMAGE                          COMMAND             CREATED
  STATUS                    PORTS
NAMES
3e524103ef68   gitlab/gitlab-ce:16.0.0-ce.0   "/assets/wrapper"   4 minutes ago
  Up 4 minutes (healthy)   22/tcp, 443/tcp, 0.0.0.0:80->80/tcp, :::80->80/tcp
distracted_heyrovsky
root@ubuntu:/home/eqst# docker exec -it 3e524103ef68 /bin/bash
root@3e524103ef68:/# gitlab-rake "gitlab:password:reset[root]"
Enter password:
Confirm password:
Password successfully updated for user with username root.
```

컨테이너 접근 명령어

패스워드 변경 명령어

그림 4. GitLab 루트 계정 패스워드 재설정

3) 취약점 테스트를 위해 PoC 가 저장된 git 파일을 공격자의 PC 로 복사한다.

PoC 가 저장된 GitHub URL 은 다음과 같다.

- URL: https://github.com/Occamsec/CVE-2023-2825.git

명령어	$ git clone https://github.com/Occamsec/CVE-2023-2825.git

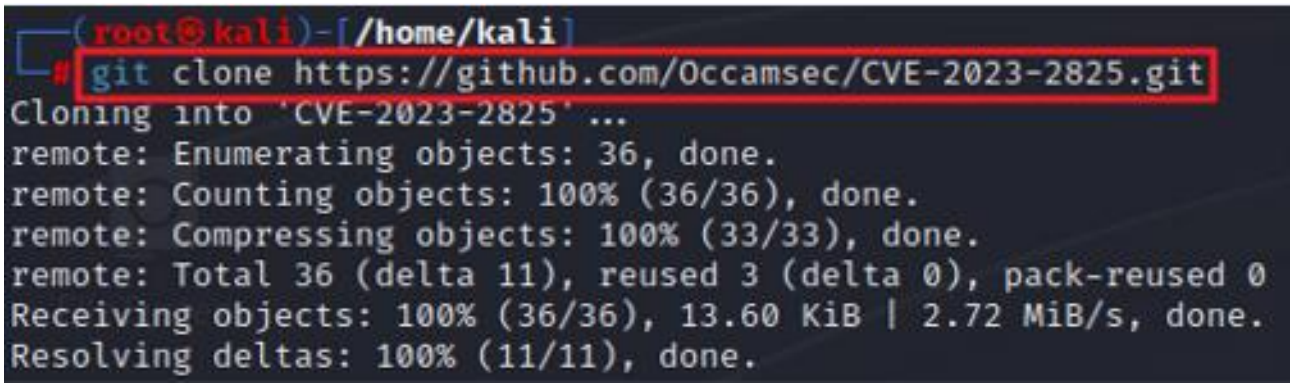


그림 5. PoC 복사 및 경로 확인

4) 편집기를 활용해 PoC 파일에 피해자 서버의 정보를 입력한다.

※ root 계정을 넣은 이유는 PoC 테스트를 위한 프로젝트 생성을 위함으로, 실제 취약점에서는 인증 정보가 없는 사용자가 공개된 프로젝트를 대상으로 공격할 수 있다.

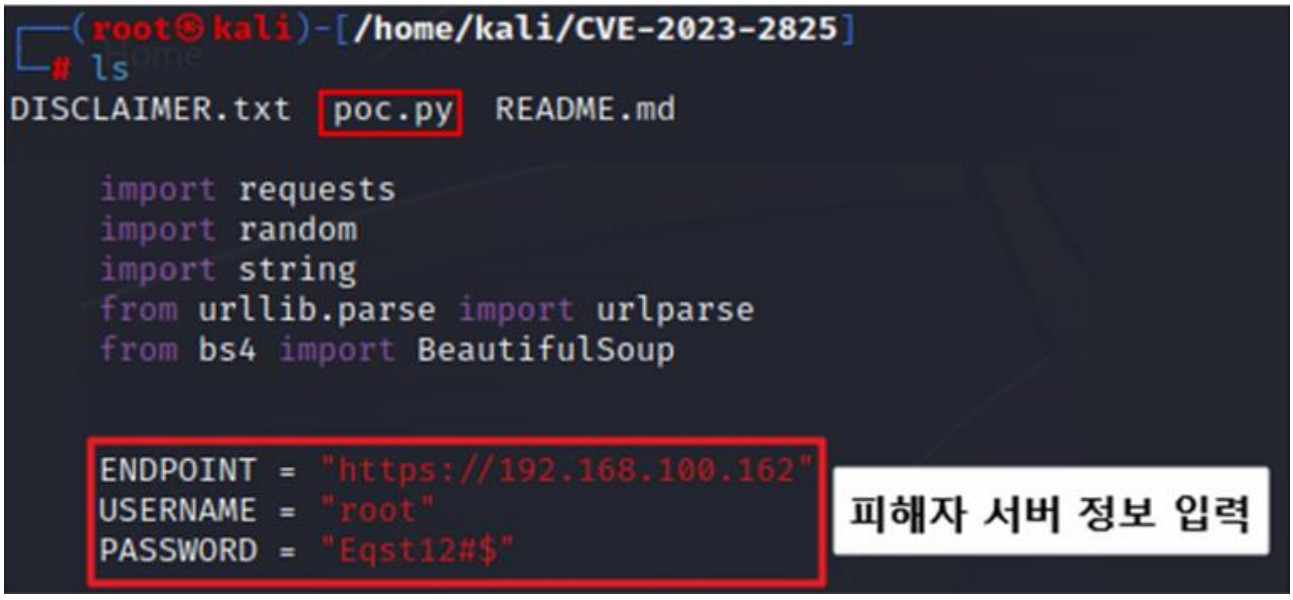


그림 6. 피해자 서버 정보 입력

5) PoC가 동작해 피해자 서버의 /etc/passwd 파일을 확인할 수 있다.

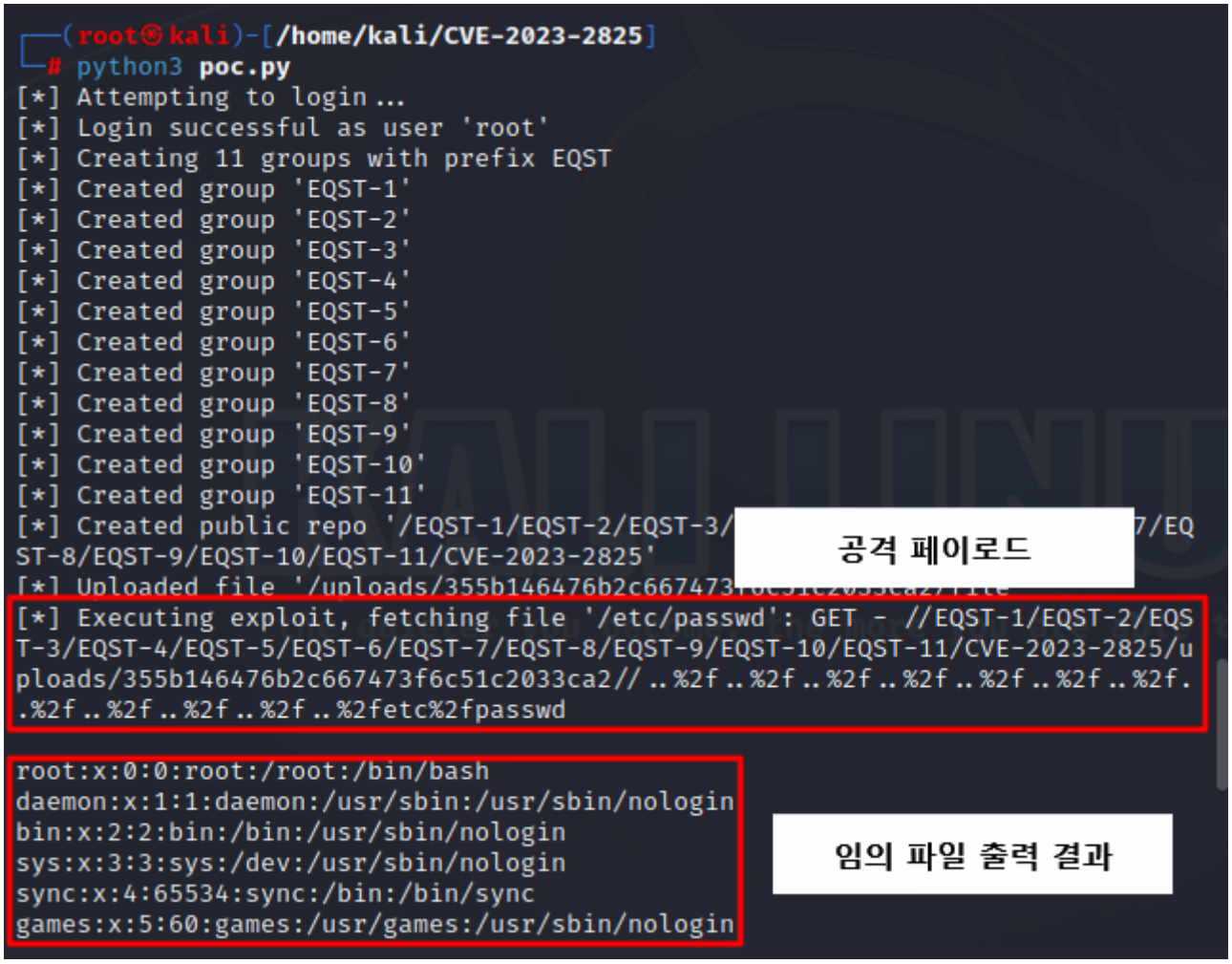


그림 7. 취약점으로 인한 임의 파일 노출

■ 취약점 상세 분석

Step 1) 취약점 개요

CVE-2023-2825 취약점은 인증되지 않은 공격자가 공개된 취약한 버전의 GitLab 프로젝트 또는 Snippet[28] 등 첨부파일에 접근할 경우 취약점이 동작한다. GitLab 서버는 요청받은 URL 경로에 파일이 존재하지 않을 경우, puma[29]로 전달 이후 디코딩하여 처리한다. 이후, GitLab 서버는 전달받은 URL 에서 파일명을 받아온다. 하지만, 파일명을 검사하는 로직이 누락되어 있어 취약점이 발생한다.

```
scope path: :uploads do
  # Note attachments and User/Group/Project/Topic avatars
  get "-/system/:model/:mounted_as/:id/:filename",
    to: "uploads#show",
    constraints: { model: %r{note|user|group|project|projects\/topic|achievements\/achievement},
    mounted_as: /avatar|attachment/, filename: %r{[^/]+} }
```

그림 8. puma 를 통한 디코딩하는 소스

공격자가 패킷을 조작해 첨부파일 명에 Path Traversal 구문을 인코딩하여 전달하면, 서버에서는 디코딩하여 처리된 문자열에서 파일명을 해석하기 때문에 취약점이 발생한다. 따라서 인코딩 문자열 "..%2f", "%2e%2e%2f"를 이용해 상위 디렉터리에 존재하는 파일에 접근할 수 있다.

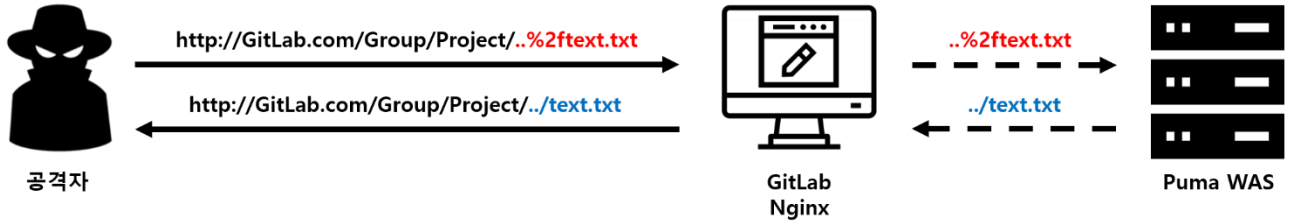


그림 9. 디코딩 해석 그림

[28] Snippet 이란 자주 사용되는 코드나 다른 사용자와 공유하기 위한 코드, 텍스트 등을 저장하기 위한 페이지다.

[29] puma 란 WAS(Web Application Server)의 한 종류로 Ruby 응용 프로그램을 위한 서버다. GitLab 의 Rails(Ruby 의 Web framework 의 일종) 응용 프로그램을 실행하기 위해 사용된다.

취약점을 이해하기 위해서는 GitLab 의 첨부파일 관련 저장 구조를 알아야 한다. 그룹의 프로젝트를 생성하거나, Snippet 을 생성할 때는 업로드 경로와 특정 디렉터리 경로가 결합되어 저장된다. 아래의 예시는 정상적으로 파일을 업로드 했을 때, 서버에 저장되는 경로이다.

업로드 파일 경로 프로젝트 생성 디렉터리 경로
/var/opt/gitlab/gitlab-rails/uploads/@hashed/[aa]/[bb]/[hash]/[hash]/[file]

그림 10. 저장되는 경로

하지만, 다운로드 요청 URL 경로에 존재하지 않은 첨부파일 다운로드 요청 시, GitLab 은 puma 서버를 통해 아래의 심볼릭 링크[30]에서 파일을 전송한다.

그림 11. 심볼릭 링크 디렉터리 경로

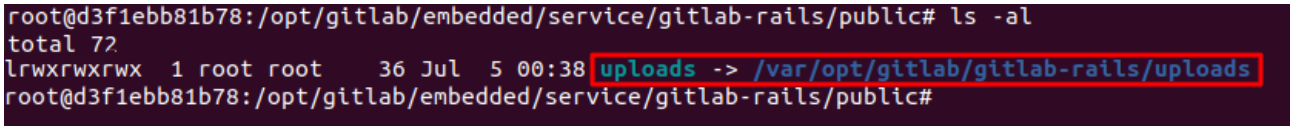


그림 12. 서버의 심볼릭 링크 경로

GitLab 의 첨부파일 업로드 시 생성되는 다운로드 요청 URL 규칙은 다음과 같다. 프로젝트에서 중첩된 하위 그룹의 생성 수만큼 디렉터리가 추가적으로 생성된다.

GitLab 주소/[Group]/[하위 그룹]/Project/uploads/[hash]/file

GitLab 주소/[Group]/[하위 그룹1][하위 그룹 2]...[하위 그룹 N]/Project/uploads/[hash]/file

그림 13. 다운로드 경로 요청 URL 구성

[30] 심볼릭 링크란 특정 파일이나 디렉터리에 대한 참조를 포함하는 파일로, Windows 운영체제의 바로 가기와 같은 기능을 한다.

하위 그룹이 하나만 존재하는 다운로드 요청 URL 일 경우는 아래의 그림과 같이 WebRoot 디렉터리인 5 개의 경로만 이동이 가능하며, 심볼릭 링크의 uploads 디렉터리까지만 이동이 가능하다.

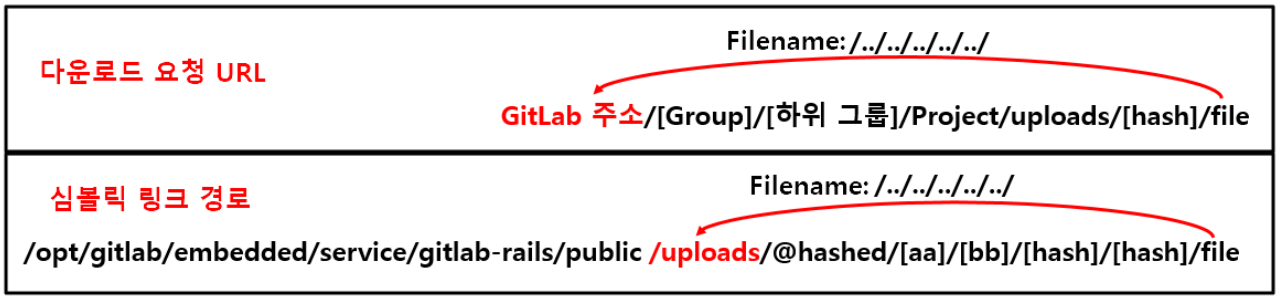


그림 14. 웹 루트 디렉터리로 이동

하지만, 다운로드 요청 URL 은 중첩된 하위 그룹의 생성 수만큼 디렉터리의 개수가 생성되고, 심볼릭 링크의 디렉터리 개수는 고정이므로, WebRoot 디렉터리 보다 상위 디렉터리까지 접근이 가능하다.

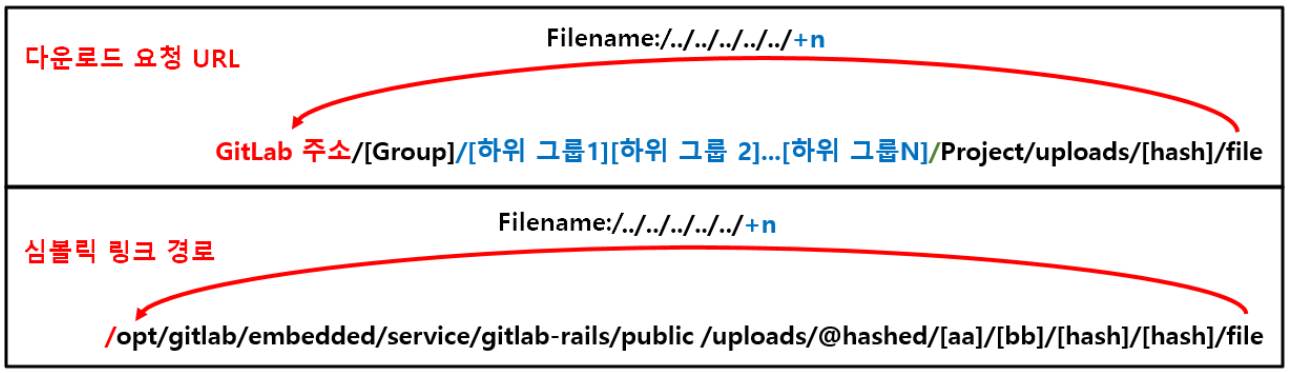


그림 15. 상위 디렉터리로 이동

서버가 첨부파일 다운로드 요청을 전달받을 때, 참조하는 심볼릭 링크의 예시를 도식화한 그림은 아래와 같다.

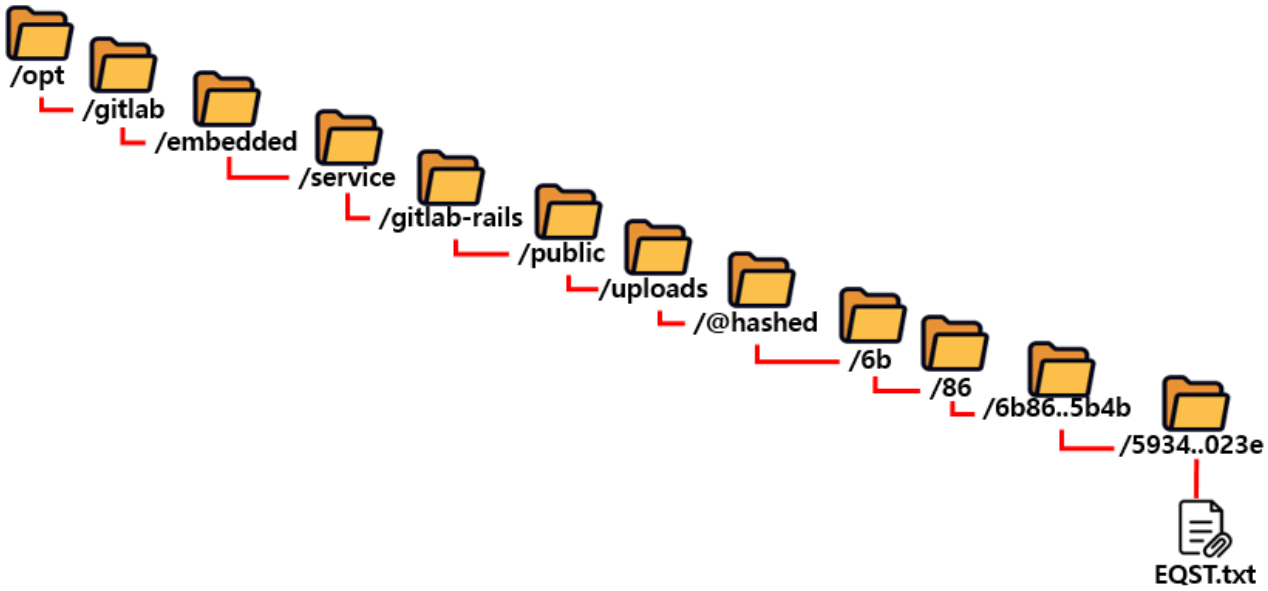


그림 16. 심볼릭 링크의 예시 도식화

Step 2) 동작 상세 분석

취약점 상세 분석을 위해 취약한 버전의 GitLab 에 그룹(EQSTLab)을 생성하고 공개 프로젝트(Insight)를 생성한다.

※ 취약점을 분석하기 위해서 현재 경로를 출력하는 print.txt 파일을 각각의 디렉터리에 생성했다.

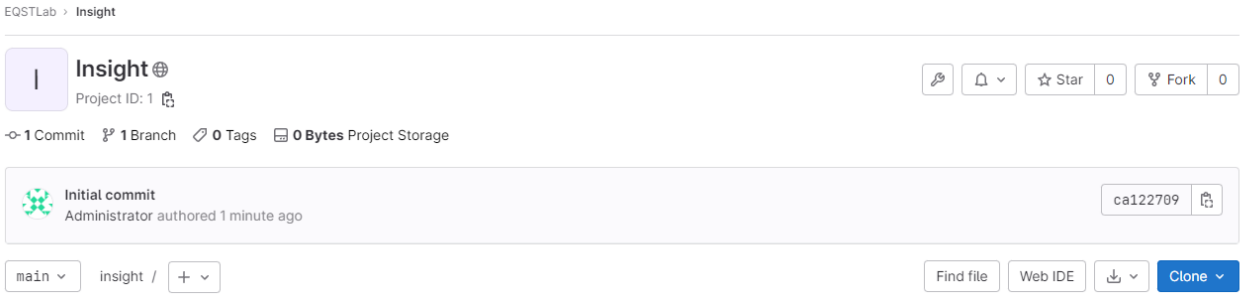


그림 17. 생성 화면

프로젝트 생성 이후, 첨부파일을 악용하기 위해서 해당 프로젝트에 관련 내용을 적을 수 있는 공간인 issue 를 생성하여 첨부파일(EQST.txt)을 업로드한다.

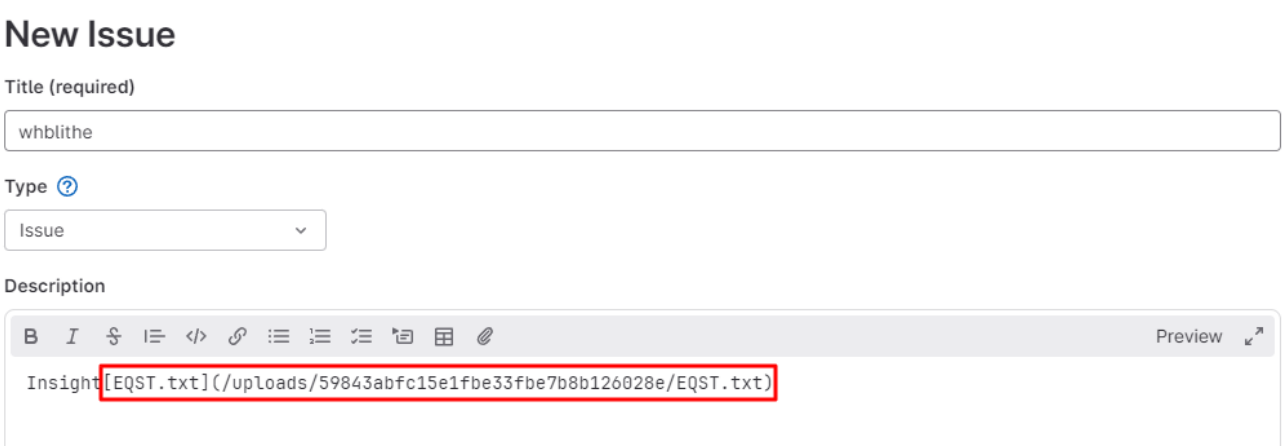


그림 18. 첨부파일 등록

아래의 경로를 통해 첨부파일(EQST.txt)를 다운로드 받는다.

- http://192.168.100.162/eqstlab/insight/uploads/59843abfc15e1fbe33fbe7b8b126028e/EQST.txt

그림 19. 파일 다운로드

CVE-2023-2825 취약점을 악용하기 위해서는 프록시 툴을 이용해, 파일명을 변조하여"../"문자열을 URL 인코딩한 후 "..%2fprint.txt" 또는 "%2e%2e%2fprint.txt" 페이로드를 피해자 서버에 전달하면 상위 경로에 도달할 수 있다.

프록시 툴을 이용해 상위 경로의 현재 경로를 출력하는 print.txt 의 응답 값은 다음과 같다.

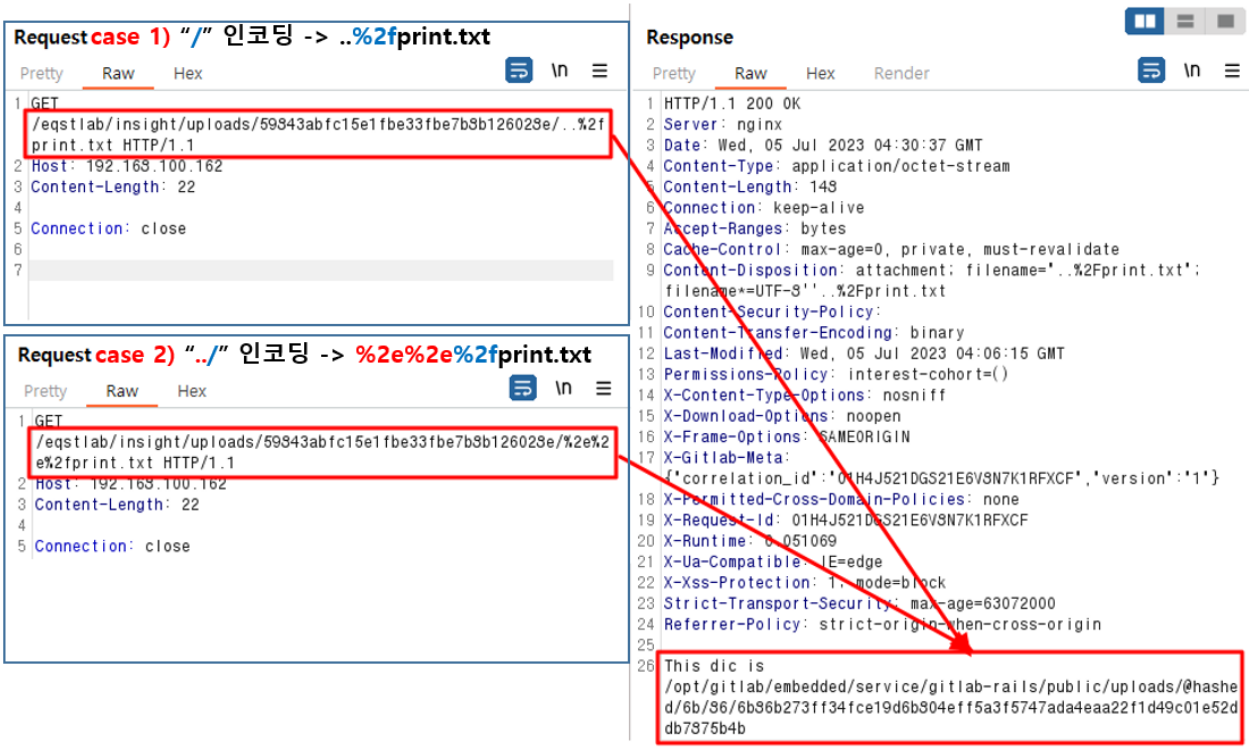


그림 20. 상위 경로로 이동 후 파일 정보 출력

한 단계씩 상위 경로로 이동을 반복하다, 상위 5 개의 디렉토리 이동할 때 400 Bad Request 에러를 반환한다. 이는 하위 그룹을 만들지 않은 프로젝트 구성이기 때문에, 다운로드 요청 URL 에는 /eqstlab/insight/uploads/59843abfc15e1fbe33fbe7b8b126028e/ 4 개의 디렉터리만 포함되어 있다. 따라서, WebRoot 디렉터리 보다 상위 디렉터리인 5 개 디렉터리 이동은 불가능하다.

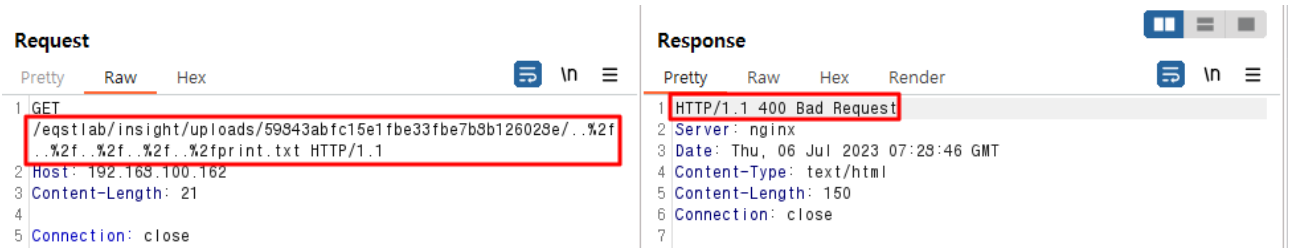


그림 21. 에러 반환

아래 그림은 WebRoot 디렉터리 보다 상위 디렉터리인 5 개의 경로를 이동 시, 400 Bad Request 에러를 반환하는 과정을 도식화한 그림이다.

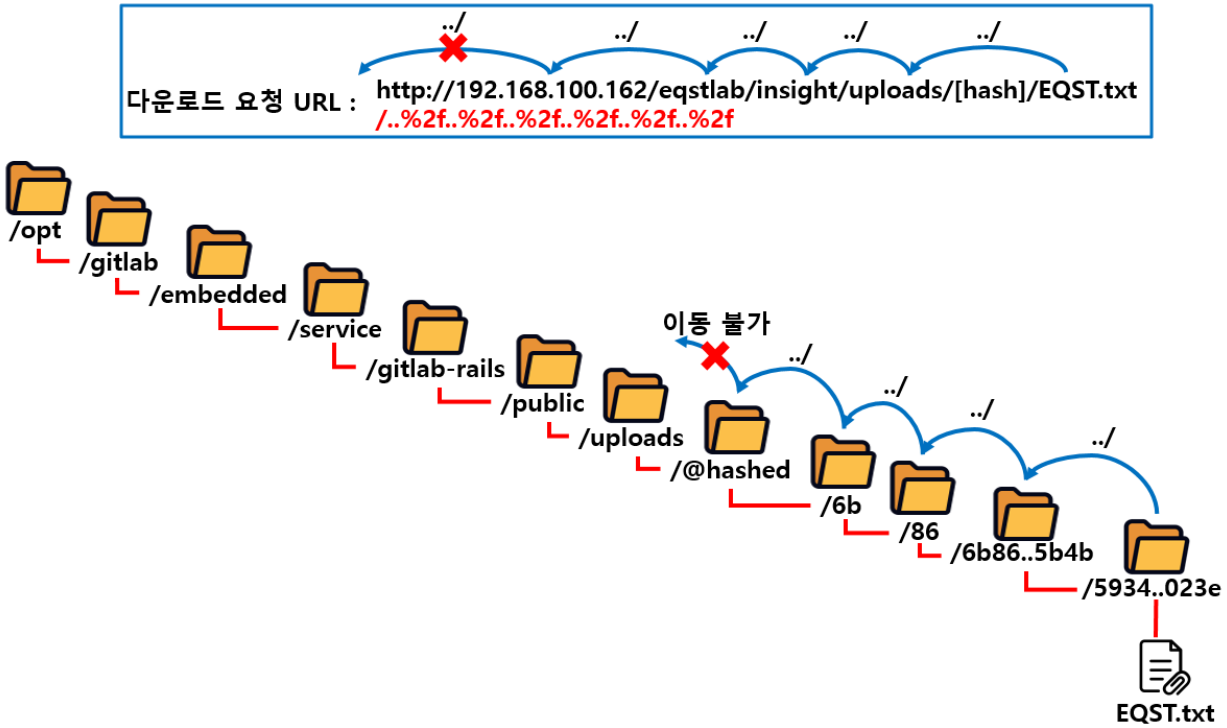


그림 22. 이동 불가 도식화

CVE-2023-2825 취약점을 활용해 WebRoot 디렉터리 보다 상위 디렉터리에 접근하기 위해서는 중첩된 하위 그룹을 추가하여, 다운로드 요청 URL 내의 포함된 디렉터리 수를 늘려야 한다.

따라서, WebRoot 보다 상위 디렉터리에 위치한 주요 정보 중 하나인 /opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml 에 접근하기 위해서는 기존의 4 개의 디렉터리에 3 개를 추가하여 총 7 개의 상위 디렉터리로 이동해야 한다. 따라서 중첩된 하위 그룹 3 개를 추가해 CVE-2023-2825 취약점을 악용한다.

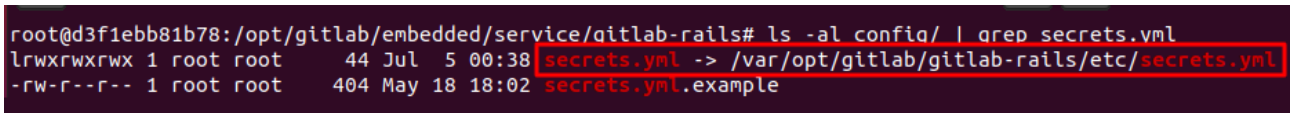


그림 23. 서버 내의 /config/secrets.yml 경로

7 개의 상위 디렉터리로 접근을 위해 3 개의 중첩된 하위 그룹을 생성한 그림은 아래와 같다.

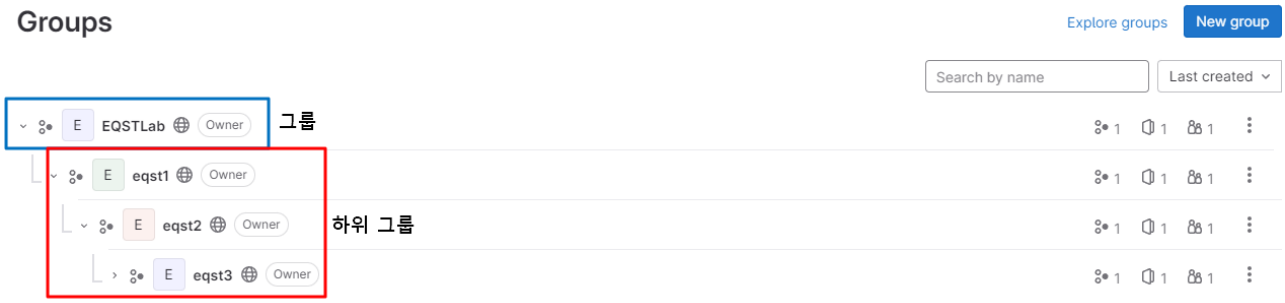


그림 24. 하위 그룹 생성

아래 그림은 중첩된 하위 그룹 3 개를 추가하여, WebRoot 디렉터리 보다 상위 디렉터리인 gitlab-rails 에 존재하는 /config/secrets.yml 파일에 접근하는 과정을 도식화한 그림이다.

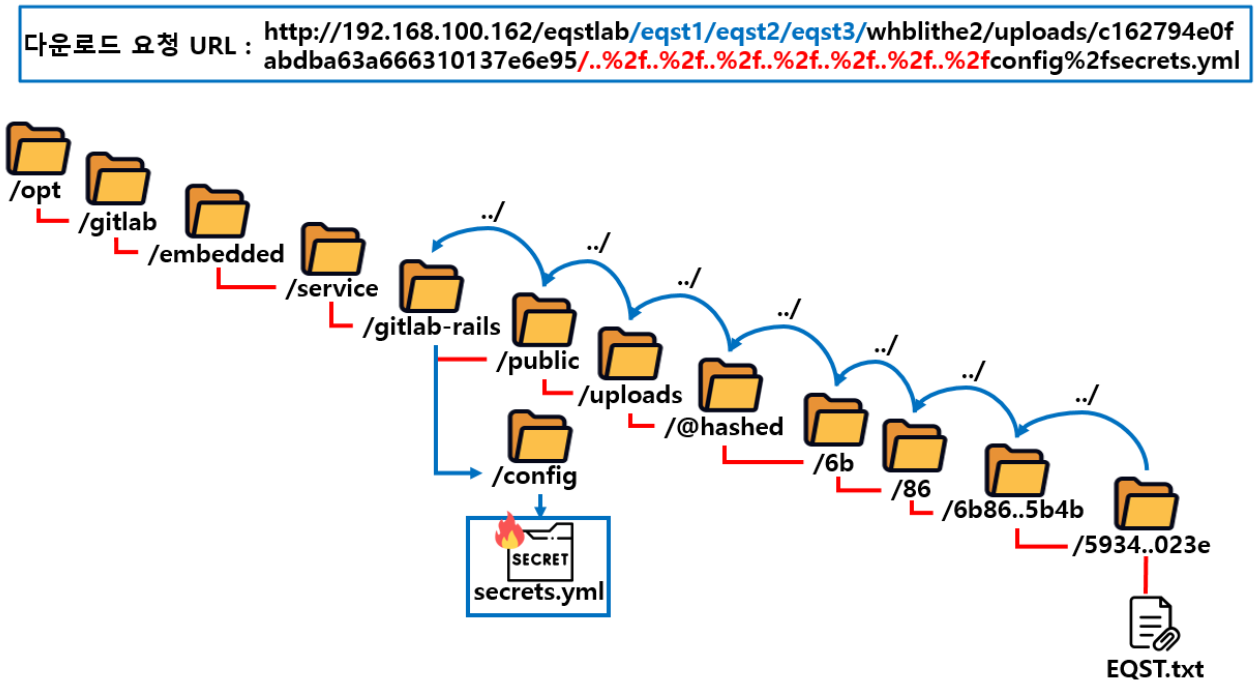


그림 25. /config/secrets.yml 접근 도식화

앞선 과정을 통해 중첩된 하위 그룹을 생성한 뒤 /config/secrets.yml 정보를 출력하는 페이로드는 아래와 같다.

그림 26. 상위 디렉터리의 /config/secrets.yml 파일 접근

따라서, 최상위 루트 디렉터리로 접근하기 위해서는 총 12 개의 상위 디렉터리로 이동해야 하므로, 1 개 그룹과 8 개의 하위 그룹 프로젝트의 첨부파일 경로를 조작해 /etc/passwd 까지 접근이 가능하다.

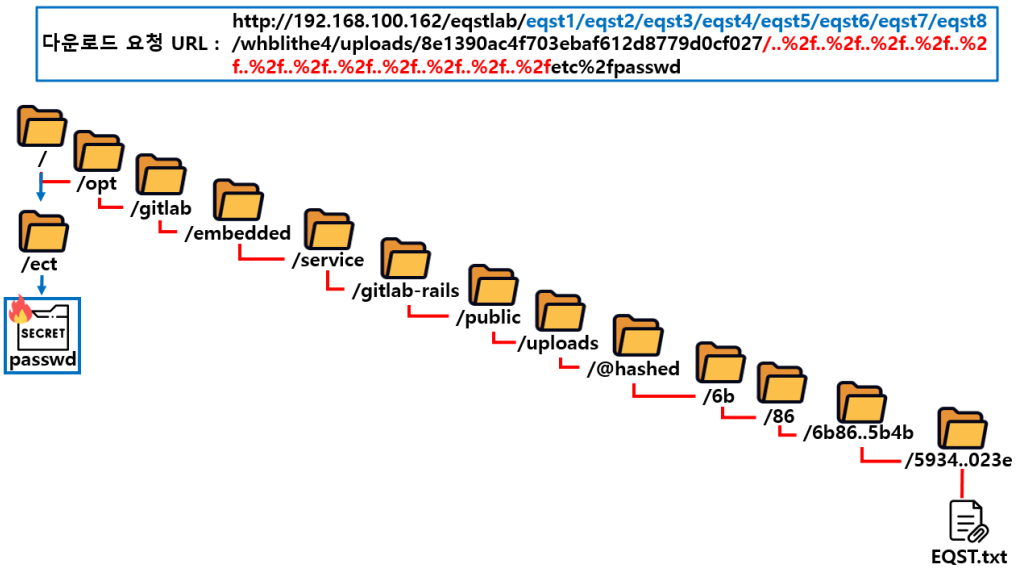


그림 27. 루트 디렉터리 접근

앞선 과정을 통해 12 개의 상위 디렉터리로 이동해 최상의 루트 디렉터리의 이동해 /etc/passwd 출력하거나 다운로드 받을 수 있다.

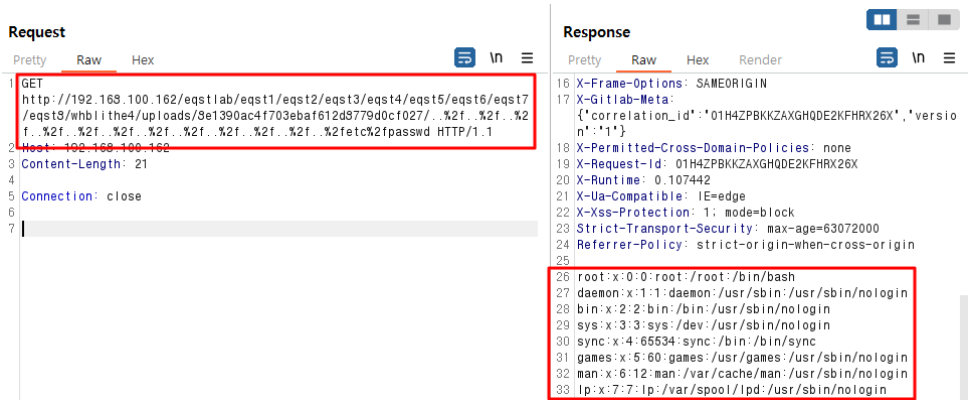


그림 28. root 폴더의 /etc/passwd 파일 정보 획득

URL 주소에 입력하면 /etc/passwd 파일을 다운로드할 수 있다.

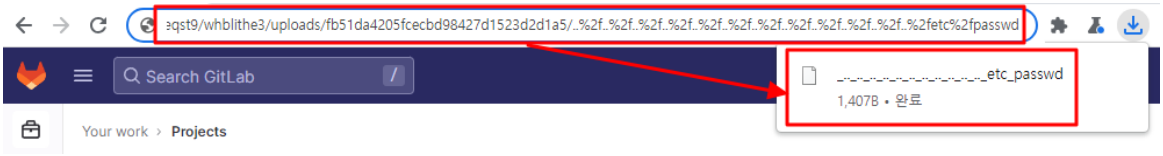


그림 29. /etc/passwd 파일 다운로드

■ 대응 방안

취약한 버전의 GitLab 서버를 운영 중이라면, 공격자가 프로젝트에 issue 를 생성하거나 공개된 Snippet 에 첨부파일을 등록하여 취약점을 악용할 수 있다. 이에 대응하기 위해서는 정규식 표현을 기반으로 디코딩한 문자열이 'Path Traversal 패턴'인지 검사하는 로직이 추가된 GitLab 16.0.1 이상 버전으로 업데이트하는 것이 안전하다.

```
def check_path_traversal!(path)
  return unless path

  path = path.to_s if path.is_a?(Gitlab::HashedPath)
  raise PathTraversalAttackError, 'Invalid path' unless path.is_a?(String)

  path = decode_path(path)
  path_regex = %r{(\A(\.{1,2})\z|\A\.\.[/\\]|[/\\]\.\.\z|[/\\]\.\.[/\\]|\n)}

  if path.match?(path_regex)
    logger.warn(message: "Potential path traversal attempt detected", path: "#{path}")
    raise PathTraversalAttackError, 'Invalid path'
  end

  path
end
```

그림 30. 정규식 표현을 통한 Path Traversal 탐지

16.0.1 이상 버전은 업로드를 관여하는 모듈에서 check_path_traversal 로직이 추가되어 Path Traversal 이 탐지될 경우 bad_reqeust 를 반환하고 있음을 확인할 수 있다.

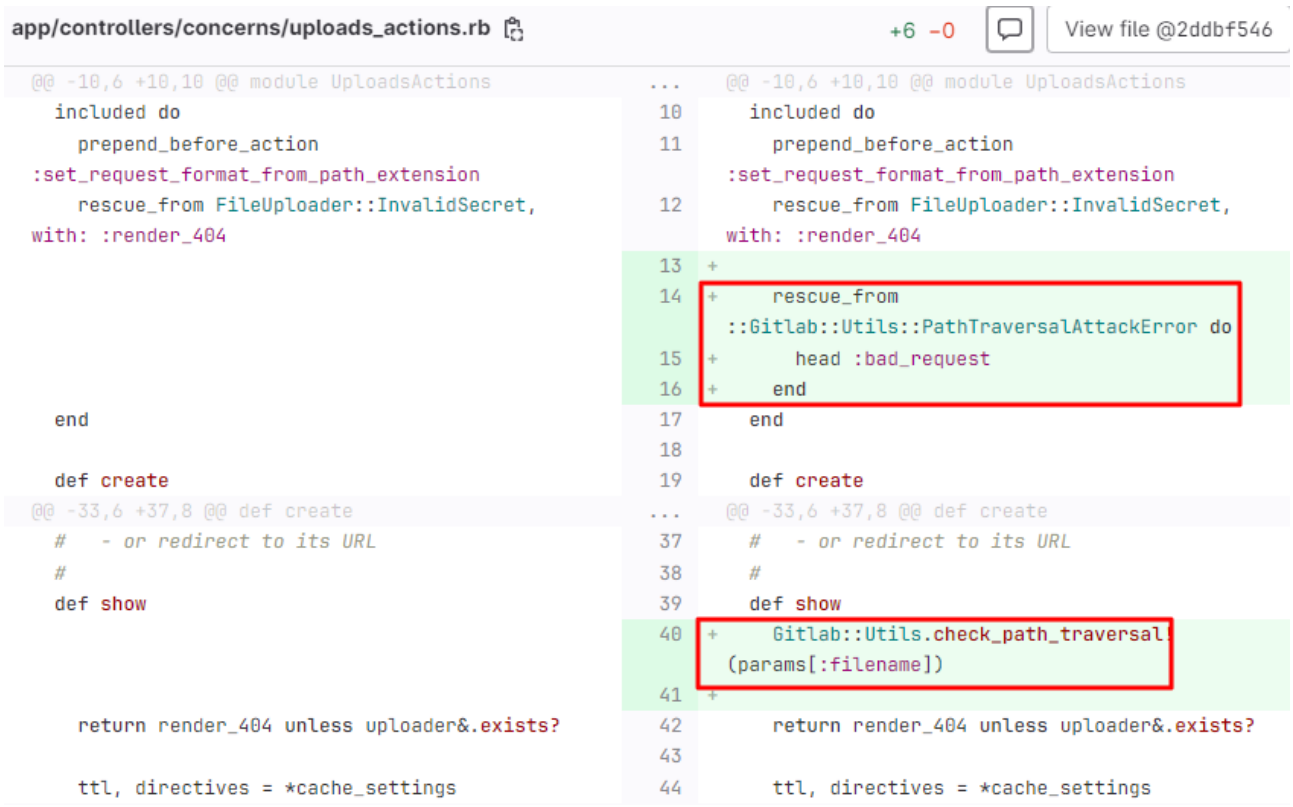


그림 31. 검사 로직 추가

불가피하게 버전 업데이트가 어려울 경우 공개된 프로젝트를 비활성화하거나, 웹 방화벽을 이용해 패킷을 검사하는 것이 필요하다. 하지만 이는 취약점에 대한 완벽한 대응 방안이 아니므로 검사 로직이 추가된 16.0.01 이상 버전으로 업데이트 하는 것을 권장한다.

■ 참고 사이트

- URL: https://labs.watchtowr.com/gitlab-arbitrary-file-read-gitlab-cve-2023-2825-analysis/
- URL: https://github.com/Occamsec/CVE-2023-2825.git
- URL: https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/

EQST INSIGHT

2023.07

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST사업그룹
제　작 : SK쉴더스 커뮤니케이션그룹