infosec

Threat Intelligence Report

EQST INSIGHT

2024

01

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

infosec

Contents

EQST insight

PCI DSS v4.0 개편에 따른 주요 보안 요구사항 분석 ---------- 1

Keep up with Ransomware

지속되는 BlackSuit 랜섬웨어 위협 ---------- 15

Research & Technique

ownCloud 정보 노출 및 인증 우회 취약점(CVE-2023-49103/ CVE-2023-49105) ------ 30

EQST insight

PCI DSS v4.0 개편에 따른 주요 보안 요구사항 분석

EQST 원격 Shared 진단팀 김종선 수석

■ 개요

PCI DSS 는 카드 결제 산업의 데이터 보안 표준(Payment Card Industry Data Security Standard)의 약자로, Global Brand 5 개사(Visa, Master, Amex, JCB, Discover)의 카드소유자데이터(이하 CHD) 보호를 위해 제정됐다.

Global Brand 5 개사는 데이터 보안의 지속적이고 체계적인 관리를 위해 PCI 보안표준위원회(이하 PCI SSC)를 설립했으며, 보안 표준 관리, PCI 보안 표준 보안 솔루션 검증, 교육, 심사원 조직 관리 등의 역할을 수행하고 있다. 2020 년에는 UnionPay 도 PCI SSC 에 참여함으로써 현재 총 6 개의 Global Brand 카드가 PCI SSC 에 참여하고 있다.

PCI DSS 는 지불 카드 계정 데이터(payment card account data)를 보호하는 것을 주된 목적으로 한다. 기업이 비즈니스 목적으로 카드 소유자의 데이터를 저장하고 처리, 전송을 필요로 하는 경우 PCI DSS 준수가 요구된다. 국내에서는 현재 카드사, VAN/PG 사, 선불카드 사업자 등 결제 비즈니스를 수행하는 기업들 외에도 여행사, 항공사, 면세점 등 다양한 업종에서 PCI DSS 인증을 취득하여 준수, 유지하고 있다.

PCI DSS 는 비즈니스 카드 결제 데이터를 처리할 때 발생할 수 있는 보안 위협을 최소화하고, 소비자의 정보를 안전하게 보호하기 위한 조치의 일환으로 이뤄지고 있다.

계정 데이터(Account Data)	
카드 소유자 데이터(Cardholder Data)	**민감한 인증 데이터(Sensitive Authentication Data)**
카드 번호 (PAN)	전체 트랙 데이터 (Full Track Data)
카드 소유자 이름 (Cardholder Name)	CVC (Card Verification Code)
유효기간 (Expiration Date)	PINs/PIN blocks
서비스 코드 (Service Code)	

출처: PCI DSS v4.0 재가공

표 1. 지불 카드 계정 데이터(payment card account data)

PCI DSS 는 결제 데이터를 보호하기 위해 설계된 12 개의 기술 및 운영 요구사항 기준을 제시하고 있다. 464 개의 세부 요건과 48 개의 부록으로 제공되고 있으며, 전체적인 보안 요구사항은 아래와 같다.

목적	PCI DSS 요구사항
안전한 네트워크 및 시스템 구축 및 유지	1. 네트워크 보안 제어 장치 설치 및 유지관리 2. 모든 시스템 구성 요소에 보안 설정 적용
계정 데이터 보호	3. 저장된 계정 데이터 보호 4. 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화로 카드 소유자 데이터 보호
취약점 관리 프로그램 유지	5. 악성 소프트웨어로부터 모든 시스템과 네트워크를 보호 6. 안전한 시스템과 소프트웨어 개발 및 유지
강력한 접근 통제 조치 구현	7. 업무상 알아야 할 필요(need to know)에 따라 시스템 구성요소 및 카드 소유자 데이터에 대한 접근 제한 8. 사용자 식별 및 시스템 구성 요소에 대한 접근 인증 9. 카드 소유자 데이터(PAN)에 대한 물리적 접근 제한
네트워크에 대한 정기적 모니터링 및 테스트	10. 시스템 구성요소 및 카드 소유자 데이터(PAN)에 대한 모든 액세스를 기록 및 모니터링 11. 시스템 및 네트워크의 보안에 대한 정기적인 테스트
정보 보안 정책 유지	12. 조직 정책 및 프로그램을 통한 정보 보안 지원

출처: PCI DSS v4.0 재가공

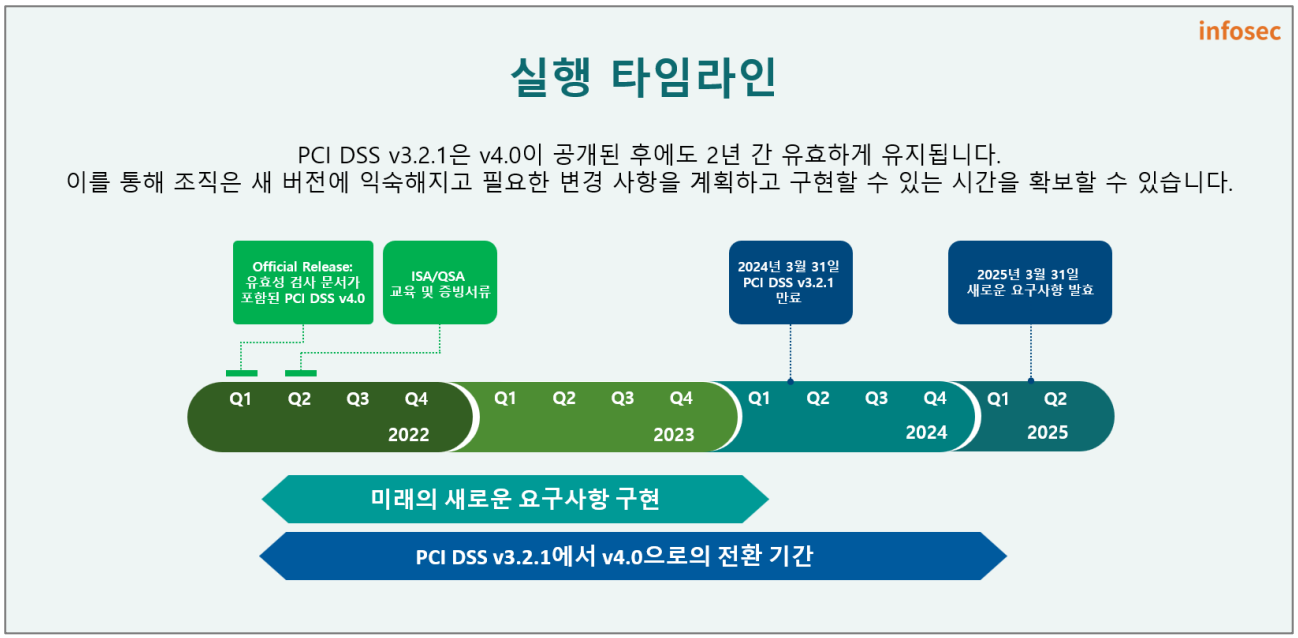
표 2. 주요 PCI DSS 요구 사항(Principal PCI DSS Requirements)

이번 헤드라인에서는 PCI DSS 버전 4.0 적용에 따른 주요 변동사항을 살펴보고, 기존 PCI DSS 를 유지하거나 새롭게 적용하고자 하는 기업 및 기관에게 유익한 정보를 제공하고자 한다. 새로운 버전의 PCI DSS 는 결제 데이터를 더욱 효과적으로 보호하고 최신 보안 표준에 부합하도록 하는데 중점을 두고 있다.

■ PCI DSS v4.0 적용 Timeline

PCI DSS v4.0 은 2022 년 3 월 31 일 발표됐다. PCI DSS 를 준수하고자 하는 기업은 2024 년 3 월 31 일까지 기존 버전(v3.2.1)과 신규 버전(v4.0)을 선택해 인증을 준비할 수 있다. 2024 년 4 월 이후로 인증을 취득하는 경우에는 반드시 PCI DSS v4.0 을 적용하여 준비해야 한다.

다만, 비용 및 리소스 부족 등의 문제로 PCI DSS v4.0 에서 발표된 대다수의 신규 보안 요건 준수가 어려운 경우, 2025 년 3 월 31 일까지는 유예기간이 적용되므로, 2025 년 4 월 전까지 적용을 완료하면 된다.



출처: PCI DSS v4.0 At a Glance 재가공

그림 1. PCI DSS v4.0 적용 Timeline

■ 주요 변동사항

PCI SSC 에 따르면, 이번 변경사항은 관련 글로벌 결제 산업계의 200 개 이상 조직으로부터 6,000 건 이상의 피드백 항목을 받아 발표됐다. 특히 진화하는 사이버 공격과 IT 기술 및 결제 산업의 변화 과정에서 보안 환경을 지속적으로 유지할 수 있도록 구성됐다. 또한, 새로운 표준은 각 조직의 환경에 따라 적용 가능하도록 유연성을 높이고 보다 견고한 검증 과정을 도입해 보안 수준을 강화했다.

1. 맞춤형 접근법(Customized Approach)과 특정 위험 분석(Targeted Risk Assessment)

신규 버전(v4.0)에서는 PCI DSS 를 구현하고 검증하는 2 가지의 접근 방식을 제시하고 있다.

첫 번째는 기존 버전(v3.2.1)부터 계속 사용되어온 전통적인 방법으로, PCI DSS 에서 정의된 요구사항과 테스트 절차를 사용하는 것으로 정의된 접근법(Defined Approach)이라고 한다. 이 방법은 명시된 요구사항을 충족하기 위해 보안 통제를 구현하고, 평가자는 해당 요구사항이 충족되었는지 확인하기 위해 정의된 테스트 절차를 따르는 것이다. 만약, 비즈니스 제약사항이나 기술적인 문제로 인해 명시적으로 PCI DSS 요구사항을 충족할 수 없는 경우, 해당 요구사항과 관련된 위험을 충분히 완화하는 대체 통제 방안(Compensation Control)을 적용할 수 있다.

두 번째 평가 방법은 맞춤형 접근법(Customized Approach)으로, 신규 버전(v4.0)에서 새롭게 도입된 방식이다. 각 PCI DSS 요구사항의 목표에 중점을 두며, 기업 또는 기관이 비즈니스의 목적과 내부 환경에 맞는 통제 절차를 구현하는 방법이다. 이 방법은 정의된 테스트 절차를 갖고 있지 않는 대신 구현된 보안 통제가 명시된 목표를 충족하는지 확인하기 위한 적합한 테스트 절차를 도출해야 한다. 기업 또는 기관은 구현된 보안 통제에 대한 위험분석을 주기적으로 수행함으로써 보안 통제의 적절성을 확보해야 한다.

맞춤형 접근법(Customized Approach)은 각 기업의 환경에 맞는 최적화된 보안 통제 방법을 적용하고 평가하기 위한 자체적인 테스트 절차를 구현하는 것으로, 이를 적용하는 경우 아래 사항들을 충족해야 한다고 명시하고 있다. (PCI DSS v4.0 요건 12.3.2)

- Appendix E1의 보안 통제 매트릭스 템플릿에 지정된 모든 정보를 포함하여 각 맞춤형 보안 통제에 대한 증거를 문서화하고 유지
- Appendix E2의 대상 위험 분석 템플릿에 지정된 모든 정보를 포함하여 각 맞춤형 보안 통제에 대한 특정 위험 분석(PCI DSS 요구 사항 12.3.2)을 수행하고 문서화
- 각 맞춤형 보안 통제에 대한 테스트를 수행하여 효율성을 입증하고 수행된 테스트, 사용된 방법, 테스트 대상, 테스트 수행 시기 및 테스트 결과를 보안 통제 매트릭스에 문서화
- 각 맞춤형 제어의 효율성에 대한 증거를 모니터링하고 유지
- 완성된 통제 매트릭스, 특정 위험 분석, 테스트 증거 및 맞춤형 제어 효과에 대한 증거를 평가자에게 제공

Appendix E1 과 E2 는 PCI SSC 에서 발행한 공식 샘플 자료이며, PCI DSS v4.0 공식 문서에서 확인이 가능하다. Appendix E1 은 맞춤형 접근법(Customized Approach)을 통해 PCI DSS 요구사항을 충족할 경우 기업 또는 기관에서 적용할 보안 통제 방법에 대해 작성해야 하는 문서 템플릿이다.

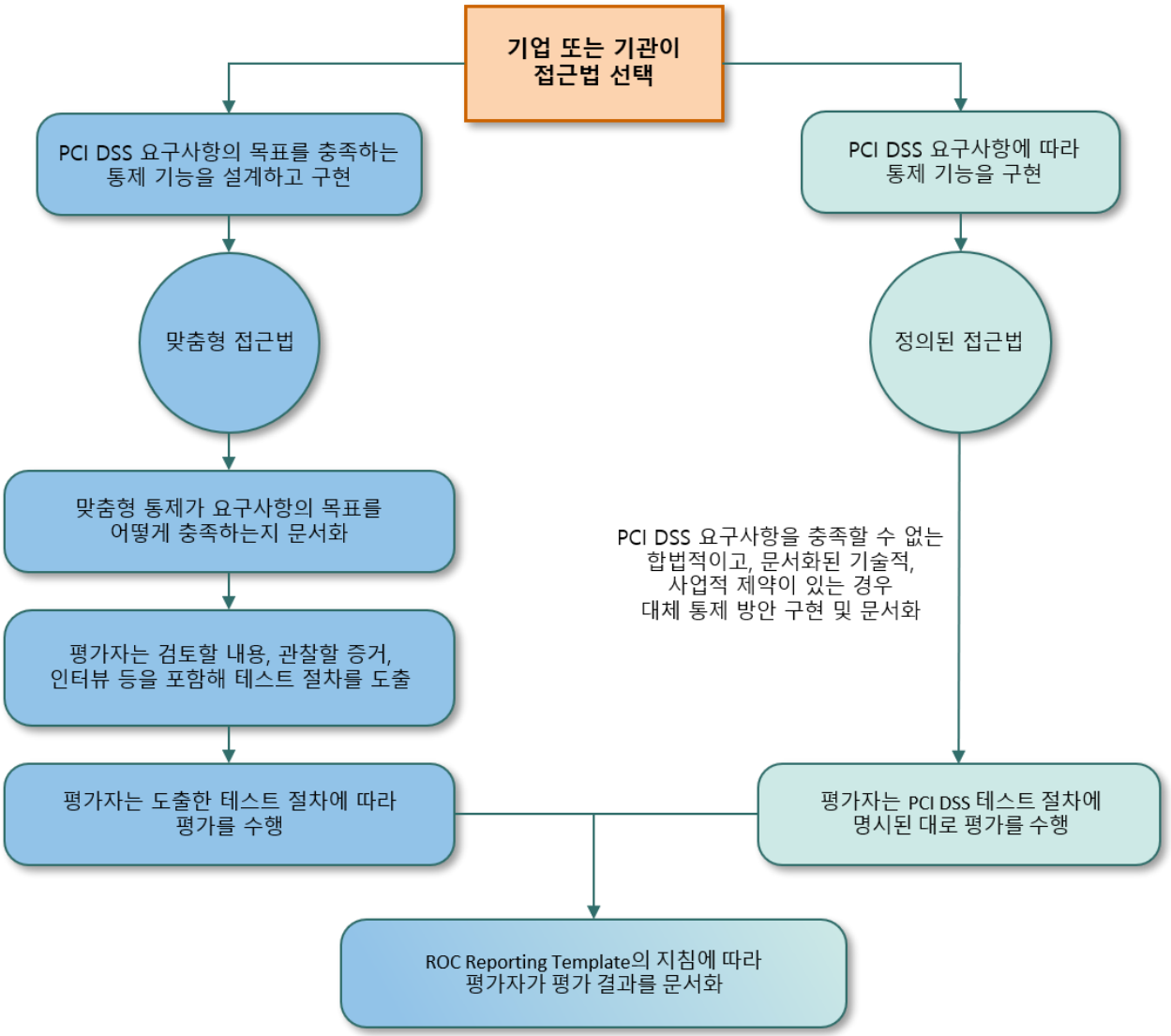
템플릿을 통해 작성이 요구되는 정보는 다음과 같다.

- 제시된 보안 통제 방법을 통해 충족되는 PCI DSS 요구사항의 번호
- 각 PCI DSS 요구사항의 목적
- 적용된 보안 통제 방법의 세부 내용
  - ✓ 통제 적용 범위, 위치, 관리 및 모니터링 참여자, 전반적인 책임자
  - ✓ 적용된 보안 통제가 어떻게 PCI DSS 요구사항의 목적을 충족시키는지에 대한 설명

Appendix E1 템플릿을 통해 맞춤형 보안 통제 절차를 마련하였다면, 해당 보안 통제를 통해 카드 계정 데이터 보안이 얼마나 강화되었는지를 평가해야 한다. 이러한 평가를 위한 템플릿을 Appendix E2 를 통해 제공하고 있다. 주요 내용은 아래와 같다.

- PCI DSS 요건 별 요구사항 미 충족 시 예상되는 피해 작성
- 정의된 접근법(Defined Approach) 적용이 불가능한 사유 작성
- 맞춤형 접근법(Customized Approach)을 통해 적용된 보안 통제를 바탕으로 어떻게 피해를 예방할 수 있는지 설명
- 적용된 보안 통제가 무력화될 수 있는 상황 식별 및 이를 예방할 수 있는 방법 설명
- 적용된 보안 통제가 정상적으로 작동하지 않는 경우를 탐지할 수 있는 기업의 프로세스와 시스템에 대한 설명
- 적용된 보안 통제의 우회 방안, 우회 방법의 난이도, 통제 작동 전 위협 행위 탐지 가능성에 대한 검토
- 정의된 접근법(Defined Approach)과 비교해 예상되는 피해의 발생 빈도 변화 검토
- 적용된 보안 통제를 통한 영향도 평가
  - ✓ 피해 규모(카드 계정 데이터 유출 건수) 축소
  - ✓ 위협 탐지, 유출된 계정 데이터에 대한 신속한 알림, 위협 행위자 격리 시간 단축 등
- 해당 위험 분석에 대한 최종 승인 및 주기적 점토

종합해보면, PCI DSS v4.0 부터 기업의 환경에 따라 PCI DSS 의 각 요구사항에 따라 정의된 접근법(Defined Approach) 또는, 맞춤형 접근법(Customized Approach)을 선택하여 사용할 수 있다. 맞춤형 접근법(Customized Approach)을 사용하여 사용자 정의 보안 통제를 사용할 경우, 주기적으로 통제 절차에 대한 검증과 위험 분석 수행 및 관리 책임자의 승인을 획득하여야 한다.



출처: PCI DSS v4.0 재가공

그림 2. PCI DSS 적용 접근 방식(PCI DSS Validation Approaches)

2. PCI DSS v4.0 의 주요 변경 사항

이번에는 신규 버전(v4.0)에 추가 또는 변경된 보안 요구사항은 다음과 같다. 이번 신규 버전(v4.0)에서는 총 464 개의 세부요건과 48 개 부록으로 이루어져 있다. 요건 통합, 분리, 번호 재지정 등의 이유로 이전 버전(v3.2.1) 보다 세부요건은 52개 늘어나고 부록은 1개 감소했다. 또한, 새로운 위협과 기술, 진화하는 결제 산업의 변화를 반영해 다음과 같은 보안 요구사항들이 추가 또는 변경되었다.

- 카드 계정 데이터(Account Data) 암호화 요건 강화
  - ✓ 디스크 또는 파티션 수준의 암호화는 이동식 디스크에 한정하여 허용
- 공개된 웹 애플리케이션 대상 자동화 탐지 메커니즘 적용
- 결제 페이지 보안 강화
  - ✓ 결제 페이지에서 사용되는 Client-Side Script 관리 강화
  - ✓ 결제 페이지 변조 감지 메커니즘 적용
- 시스템 계정을 포함한 모든 사용자 계정에 대한 접근 권한 검토
- 일일 단위 감사로그 검토 시 자동화 메커니즘 적용
- 네트워크 취약점 스캔 시 인증된 스캔 수행
- 사용중인 HW, SW 및 암호화 알고리즘 등에 대한 EoS, EoL등 문서화, 대응계획 수립

1) 카드 계정 데이터 암호화 요건 강화(PCI DSS v4.0 요건 3.5.2.1)

PCI DSS v4.0 부터는 카드 계정 데이터 암호화 저장 시, 파티션 단위 또는 디스크 단위 암호화는 더 이상 암호화 메커니즘으로 인정하지 않는다. 다만, 이동식 보안 USB 와 같이 OS Level 과 별개로 인증 절차를 요구하는 경우에는 허용하고 있다. 많은 기업들이 Tablespace 단위 암호화, 또는 파티션 단위 암호화를 적용하고 있는데, 해당 요건이 의무적 효력이 발생하는 2025 년 4 월 이후로는 추가적인 데이터 보호 조치가 필요하다. 데이터 보호 조치는 요건 3.5.1 에 다음과 같이 명시되어 있다.

- One Way Hash Algorithm 적용(강력한 해시 알고리즘 적용)
- Truncation(PAN 16자리 중 일부를 마스킹 적용하여 저장)
  - ✓ Truncated PAN과 Hashed PAN을 같은 공간에 저장 금지
- Index Token화 하여 저장
- 암호화 저장(강력한 암호 알고리즘 이용)

2) 공개된 웹 애플리케이션 대상 자동화 탐지 메커니즘 적용(PCI DSS v4.0 요건 6.4.2)

PCI DSS v3.2.1 까지는 공개된 웹 애플리케이션을 대상으로 1 년에 한 번씩 자동화된 웹 취약점 스캔 수행 또는 웹 방화벽과 같은 자동화된 공격 탐지 메커니즘을 적용하도록 요구했으나, 신규 버전(v4.0) 부터는 자동화된 공격 탐지 메커니즘을 의무적으로 요구하고 있다.

3) 결제 페이지 보안 강화(PCI DSS v4.0 요건 6.4.3, 11.6.1)

결제 페이지에 한정해, PCI DSS v4.0 에 새롭게 추가된 요구사항이다.

- 결제 페이지에 사용되는 Client-Side Script 목록화
  - ✓ 각 스크립트 별 사용되는 목적 명시, 관리자 승인 필요
  - ✓ 사용되는 스크립트의 무결성 검증 메커니즘 적용
- 결제 페이지에 대한 위변조 방지 메커니즘 적용
  - ✓ 위변조 발생 시 즉시 담당자에게 Alert

jquery[1]와 같이 범용적으로 사용되는 Client-Side Script 등 외부 공급망 공격에 따른 보안 이슈에 대비했으며, 또한 카드 계정 데이터(Account Data)가 직접적으로 입력, 처리되는 결제 페이지에 대해 보안성을 강화했다.

4) 시스템 계정을 포함한 모든 사용자 계정에 대한 접근 권한 검토(PCI DSS v4.0 요건 7.2.4, 7.2.5.1)

사용자 계정 생성 시에는 다수의 기업들이 사용자 권한의 적절성 검토를 거친 후 내부 승인 절차에 의해 관리되고 있다. 다만, 해당 사용자가 퇴직 또는 부서 이동을 통해 더 이상 사용하지 않을 때, 권한 관리가 미흡한 경우가 많다. 또한, 시스템 계정의 경우 다수의 애플리케이션 또는 배치 스크립트 등과 연동되어 한번 생성되면 거의 변경하지 않는 경우가 많다.

PCI DSS v4.0 에서는 이러한 보안 결함을 줄이기 위해 모든 사용자 계정의 권한에 대해 6 개월에 1 번씩 검토를 수행해야 한다. 또한 시스템 계정에 대해 특정 위험 분석(Targeted Risk Assessment)을 통해 기업 내부에서 정한 기간에 맞게 권한 검토할 것을 요구하고 있다.

1 jquery: 웹 프론트엔드 분야에서 많이 사용되는 오픈소스 라이브러리

5) 일일 단위 감사로그 검토 시 자동화 메커니즘 적용(PCI DSS v4.0 요건 10.4.1.1)

기존 PCI DSS 버전부터 이미 인증 범위 내 모든 시스템 구성요소의 감사로그에 대한 일일 모니터링 요구사항은 존재하고 있었으나, 모니터링 방식에 대해 세부적인 가이드를 제시하지는 않았다.

그러나 최근 모니터링 대상이 되는 시스템의 수와 감사로그가 늘어남에 따라, 사람이 수동으로 모니터링을 하는 것으로 의미 있는 결과를 도출하기가 어려워진 상황이다. 이에 신규 버전에서는 모든 보안 이벤트 및 감사로그 검토 시 자동화 메커니즘을 적용할 것을 요구하고 있다.

다행인 것은 기술의 발달로 인해 SIEM 장비 등을 통해 대용량 로그에 대해 자동화 검토가 가능하며, 모니터링 해야 할 위협에 대해 Rule-Set 형태로 패턴을 생성할 수 있어 다양한 관점으로 모니터링 할 수 있다는 것이다. 이를 활용해 기업은 서비스 및 환경에 맞춤형 위협 패턴을 정의하고 자동화된 모니터링 및 변화하는 위협에 따라 Rule-Set 을 지속적으로 변경 및 최적화해야 한다.

6) 네트워크 취약점 스캔 시 인증된 스캔 수행(PCI DSS v4.0 요건 11.3.1.2)

이미 기존 PCI DSS 버전에서 네트워크 기반의 취약점 스캔을 분기별로 요구하고 있었으며, 많은 기업이 Nmap Script Engine(NSE), 또는 Nessus, OpenVAS 와 같은 Tool 을 이용해 취약점 스캔을 수행하고 있었다. 그러나 Remote Host 에서 수행함에 따라 각 시스템에 열려 있는 서비스(Port Listening 상태의 서비스)에 대해서만 제한적으로 취약점 스캔이 가능하다는 한계가 존재했다.

PCI DSS v4.0 에서는 이러한 한계점을 극복하기 위해 기존의 취약점 스캔 프로세스에 인증과정을 추가해, 각 시스템에 열려 있는 서비스뿐 아니라 모든 정보를 포함한 취약점 스캔을 요구하고 있다.

이를 수행하려면 기존의 취약점 스캔 도구에 인증정보를 미리 입력하여 인증된 스캔을 수행할 수도 있으나 실제 운영되는 시스템의 민감도에 따라 장애 발생 등의 위험이 예상되므로, 각 시스템의 모든 취약점을 식별한다는 목적을 충족하는 맞춤형 접근법(Customized Approach)을 적용하는 것이 더 나은 대안이 될 수 있다.

7) 사용중인 HW, SW 및 암호화 알고리즘 등에 대한 EoS, EoL 등 문서화, 대응계획 수립(PCI DSS v4.0 요건 12.3.3, 12.3.4)

PCI DSS v4.0 에서는 매년 주기적으로 인증 범위 내에서 사용하는 HW, SW 및 암호화 알고리즘의 동향을 파악하고 제조사의 EoS, EoL 발표 및 알고리즘 사용 만료 등의 이벤트 발생 시 신규 제품 도입, 알고리즘 변경 작업계획 등의 대응계획을 수립하도록 경영진에게 요구하고 있다.

SK 쉴더스가 다년간 외부 기관 컨설팅 또는 인증심사를 진행한 결과, 아직도 많은 기업에서 만료된 암호화 알고리즘, Eos, EoL 상태의 HW, SW 를 많이 사용하고 있는 것으로 파악됐다.

무엇보다 요건에 대해 효과적으로 대응하기 위해서는 내부 자산 현황을 상세히 파악하고 있어야 한다. 단순히 자산의 IP, OS 정보 정도만 기록하는 것이 아니라 각 시스템 별 사용되는 서비스 데몬 종류, 버전 정보, 중요 정보 저장, 전송 시에 사용되는 암호화 프로토콜 및 알고리즘 등을 상세히 파악해 자산 현황을 관리해야 한다.

■ 맺음말

지금까지 PCI DSS v4.0 개편에 따른 주요 변동사항에 대해 알아봤다.

PCI DSS v4.0 은 새로운 위협과 기술, 결제 산업의 변화를 반영해 맞춤형 접근법(Customized Approach)과 특정 위험 분석(Targeted Risk Assessment) 등을 통해 각 기업의 환경에 맞는 보안 통제를 구현할 수 있도록 유연성을 제공했다는 특징을 지닌다.

이번 헤드라인에서는 일부 변경 및 추가된 요건에 대해서만 다뤘지만, PCI DSS v4.0 전체적인 변경사항을 확인하고자 한다면 다음 자료를 통해 확인이 가능하다.

- PCI DSS v4.0 전체 요구사항 다운로드
  - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
- PCI DSS 변동사항 요약자료
  - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf

사내 보안 전담 인력 부재 등의 이유로 PCI DSS v4.0 인증을 준비하기 어려울 경우, SK 쉴더스의 MDR 서비스를 활용한다면 PCI DSS 인증에 도움이 될 수 있을 것이다. 새로운 취약점들이 꾸준히 발견되고 있는 만큼 카드, 결제 데이터와 같은 민감한 정보를 처리하는 기업에서는 실시간 모니터링과 정기적인 모의 테스트, 보안 점검 등을 해야 한다.

SK 쉴더스 MDR 서비스는 기술과 프로세스, 전문 지식 등을 결합해 24x7 위협 모니터링, 분석, 사고 대응 및 보고를 제공하는 고도화된 사이버 보안 서비스다. 특히, 보안 위협을 실시간으로 감지하고 신속한 대응 체제를 보유하고 있어 고객사가 PCI DSS 인증을 충족할 수 있도록 돕는다. SK 쉴더스는 최고 수준의 사이버 보안 및 컨설팅 전문가를 보유하고 있으며, 고객사 특성에 적합한 맞춤형 서비스를 통해 다양한 컴플라이언스 요구사항을 지원한다. 관련한 자세한 내용은 SK 쉴더스 공식 블로그를 통해 확인할 수 있다.

Keep up with Ransomware

지속되는 BlackSuit 랜섬웨어 위협

■ 개요

2023 년 12 월 랜섬웨어 공격으로 인한 피해 사례 발생 건수는 전월(497 건) 대비 약 15% 감소한 420 건으로 나타났다. 이번 달에도 많은 랜섬웨어 이슈들이 발생했는데, 그중에서도 주목할 이슈는 대표적인 RaaS(Ransomware-as-a-Service) 그룹인 BlackCat(Alphv)의 랜섬웨어 인프라가 FBI 국제 공조에 의해 상당 부분 무력화된 것이다. BlackCat(Alphv)은 전 세계적인 악명을 떨치고 있는 랜섬웨어 그룹으로 과거 Colonial Pipeline 을 공격했던 Darkside 가 전신이다. 이들은 1,000 개가 넘는 기업과 기관을 대상으로 데이터를 탈취해왔으며, 피해자들로부터 갈취한 범죄 수익은 3 억 달러(한화 약 3950 억 원)에 이른다.

FBI 는 이번 국제 공조를 통해 BlackCat(Alphv)의 네트워크 및 다크웹 사이트 일부를 폐쇄시키고 이들이 주로 사용하는 **랜섬웨어 복호화 키**를 확보했다. 이로써 BlackCat(Alphv)의 공격으로 피해를 입었던 400 여 개의 학교 와 병원 등의 주요 기반 시설에서 복구 금액인 약 6,800 만 달러(한화 약 886 억 원)를 지불하지 않고도 랜섬웨어에 의해 피해를 입었던 인프라를 복구할 수 있게 됐다. 그러나 BlackCat(Alphv)은 이를 단순 호스팅 문제라고 주장하며 다크웹 유출 사이트를 다시 오픈했으며, 계열사들에게 병원 및 원자력 발전소와 같은 민감한 인프라를 대상으로도 공격 수행을 허가하는 취지의 공지사항을 게시했다. 이후 또다시 FBI 가 유출 사이트를 압수했지만, 이들은 계속해서 다른 도메인을 통해 유출 사이트를 오픈하고 여러 대상을 타깃으로 공격을 수행하고 있다는 글을 게시하고 있다.

한편, BlackCat(Alphv)이 어려움을 겪는 동안 또 다른 주요 랜섬웨어 그룹 LockBit 이 BlackCat(Alphv)의 계열사에 LockBit 으로 합류할 것을 제안한 정황이 확인됐다. 실제로 BlackCat(Alphv)의 공격 사례로 게시됐던 독일 에너지청 관련 자료가 LockBit 의 다크웹 사이트에 등록되기도 했다. BlackCat(Alphv) 그룹은 최근 사건을 언급하며 LockBit 에 대한 감사를 표현하는 게시글을 XSS(Cross-Site Scripting) 포럼[2]에 작성했다. LockBit 또한 카르텔 형성의 필요성을 언급하며 응원의 메시지와 협력이 필요하다고 전했다.

[2] XSS 포럼 : 해킹 도구를 팔거나 관련 정보를 주고받는 다크웹 포럼

최근 글로벌 법 집행기관들의 협력으로 인해 많은 랜섬웨어 그룹들이 압박 받아 사라지고 있다. 이러한 상황은 주요 랜섬웨어 그룹들의 경각심을 불러일으키고 있다. 이번 계기로 랜섬웨어 카르텔이 형성된다면 전술, 전략적 변화가 발생할 수 있으며, 이로 인한 위협이 급증할 수 있다. 이를 미리 예방하고 대응하기 위해서는 선제적이고 통합적인 대응이 필요하다.

협력 관계를 조성하기 위한 움직임은 다른 랜섬웨어 그룹들에서도 확인되고 있다. 최근 BianLian 과 White Rabbit, Mario 랜섬웨어 그룹이 공동으로 APAC(Asia-Pacific) 지역의 금융 기관을 목표로 특정 해상 물류 회사의 비즈니스 계정을 해킹하여 악성 이메일을 배포하는 BEC(Business Email Compromise)[3] 공격을 수행한 것이 확인됐다. 동시에 이들은 중국, 대만, 태국, 한국, 인도 등의 IP 를 악용하여 비밀번호 Brute Force Attack[4]을 통한 Microsoft Exchange 서버 해킹을 시도하기도 했다. 이로 인해 랜섬웨어 감염과 데이터 탈취 등의 피해가 발생했으며, 피해 기업들은 금전을 요구하는 협박성 이메일과 전화에 시달렸다.

앞으로 랜섬웨어 그룹 간의 협력은 더욱 늘어날 것으로 예상된다. FBI 를 비롯한 국제 수사 기관이 기존의 IP 차단과 같은 완화적인 대응을 넘어 공격자들의 근거지를 직접 타격하는 방식의 움직임을 보이고 있기 때문이다. 또한, IAB(Initial Access Broker)[5]의 중요성이 강조됨에 따라 이들과 협력하는 랜섬웨어 그룹들이 늘어나고 있으며, 서로의 공격 전략과 인프라가 겹쳐 협력하는 상황이 발생할 것으로 보인다.

이 밖에도 Royal 에서 BlackSuit 로 리브랜딩 한 랜섬웨어 그룹이 국내 A 기업을 공격한 것으로 확인됐다. BlackSuit 가 다크웹 유출 사이트에 게시한 데이터에는 고객의 개인 정보도 포함되어 있어 해당 서비스 이용자들은 피싱이나 스미싱과 같은 추가적인 범죄에 노출될 수 있어 주의가 필요하다. 실제로 개인 정보가 노출된 일부 피해자들이 유출 사건을 언급하며 사과의 뜻으로 주식을 선물하겠다는 취지의 피싱 문자를 수신한 것으로 확인됐다. 이러한 피싱 문자를 수신했을 경우, 수사 기관에 신고 혹은 삭제하여 2 차 피해를 예방하고, 확인이 어려운 상황일 경우 관련 기관에 문의하는 등 주의해야 한다. BlackSuit 는 해당 기업을 포함해 12 월에만 건설, 교육, 유통 등 국내외 5 개 기업의 유출 데이터를 게시했다.

[3] BEC : 공격자가 신뢰할 수 있는 인물로 가장하여 이메일을 통해 돈이나 기밀 정보를 요구하는 행위

[4] Brute Force Attack : 가능한 모든 조합을 시도하여 비밀번호를 해독하는 무차별 대입 공격 기법

[5] IAB : 초기 침투 경로를 판매하는 개인 혹은 집단

■ 랜섬웨어 뉴스

infosec

중국, ChatGPT를 악용해 랜섬웨어 공격에 사용한 공격자 4명 체포

- ChatGPT를 통해 랜섬웨어를 개발한 혐의로 4명을 체포
- 중국 A회사 시스템에 랜섬웨어 공격 후, 몸값으로 20,000 Tether(한화 약 2,640만 원) 요구
- 체포된 공격자들은 랜섬웨어 개발, 최적화 과정에서 ChatGPT 사용

BlackCat(Alphv) 다크웹 유출 사이트, FBI에 의해 폐쇄

- BlackCat(Alphv)은 그간 1,000여개의 조직으로부터 3억 달러(한화 약 3,950억 원)의 몸값을 갈취
- FBI는 복호화 도구를 손에 넣어 400여개의 조직에 대해 무료로 복호화 서비스 제공
- BlackCat(Alphv)과 수사기관이 실랑이를 벌이며 유출 사이트 폐쇄와 복구를 반복

BlackBasta 랜섬웨어의 결함을 통해 복호화 도구 개발

- BlackBasta 랜섬웨어 피해 복구를 돕는 복호화 도구, 독일 SRLabs에서 출시
- BlackBasta 측은 결함을 인지하고 새롭게 수정된 랜섬웨어를 배포

핵티비즘 그룹 SiegedSec, 다크웹 유출 사이트 폐쇄

- 2022년 2월부터 활동을 개시한 친 러시아 성향의 핵티비즘 그룹 SiegedSec의 다크웹 유출 사이트 폐쇄
- SiegedSec은 GhostSec과 같이 다른 핵티비즘 그룹과도 제휴를 맺는 등 활발한 활동을 지속해 옴

DragonForce, 야쿠르트 호주 지사를 비롯한 21개 조직 공격

- DragonForce는 12월 20일 유출 사이트에 야쿠르트 호주 지사에 대한 공격을 주장 후 95GB 상당의 데이터 유출
- 12월에 처음 발견된 그룹으로, 핵티비스트 그룹인 DragonForce Malaysia와는 연관성이 밝혀지지 않음
- 이외에도 제조, 건설, 유통 등의 다양한 산업군에 대한 공격을 수행

Werewolves, 다양한 산업군에 걸친 공격 수행하여 23개 조직 침해 주장

- 12월에 처음 발견된 Werewolves는 러시아어로 작성된 서피스 웹 사이트를 운영
- 자체 버그바운티를 운영하며, 전 세계 기업의 사이버 보안을 강화하는 것을 사명이라고 주장

* 서피스 웹 : 검색엔진으로 찾을 수 있는 일반적인 웹 사이트

RansomedVC의 계보를 잇는 신규 랜섬웨어 그룹 Raznatovic 등장

- 12월에 처음 발견된 Raznatovic는 RansomedVC의 인프라를 구매한 것으로 추정
- 다크웹 유출 사이트에 5개의 조직에 대한 게시글을 업로드하였으나 현재는 접속 불가

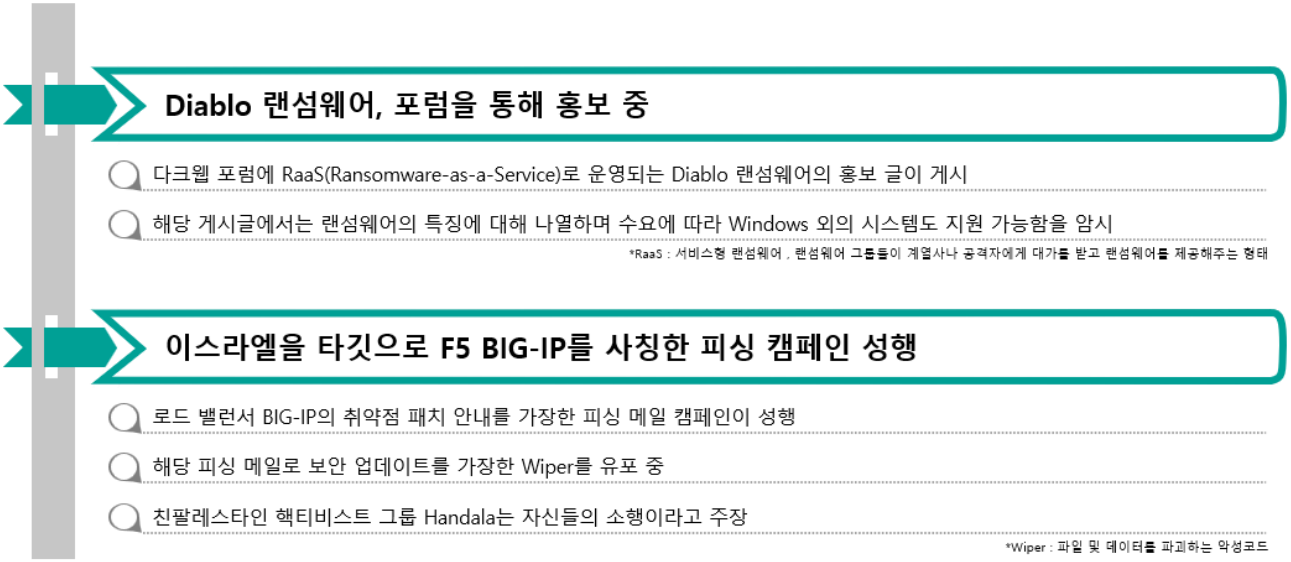

Diablo 랜섬웨어, 포럼을 통해 홍보 중
다크웹 포럼에 RaaS(Ransomware-as-a-Service)로 운영되는 Diablo 랜섬웨어의 홍보 글이 게시
해당 게시글에서는 랜섬웨어의 특징에 대해 나열하며 수요에 따라 Windows 외의 시스템도 지원 가능함을 암시
*RaaS : 서비스형 랜섬웨어 , 랜섬웨어 그룹들이 계열사나 공격자에게 대가를 받고 랜섬웨어를 제공해주는 형태
이스라엘을 타깃으로 F5 BIG-IP를 사칭한 피싱 캠페인 성행
로드 밸런서 BIG-IP의 취약점 패치 안내를 가장한 피싱 메일 캠페인이 성행
해당 피싱 메일로 보안 업데이트를 가장한 Wiper를 유포 중
친팔레스타인 핵티비스트 그룹 Handala는 자신들의 소행이라고 주장
*Wiper : 파일 및 데이터를 파괴하는 악성코드

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

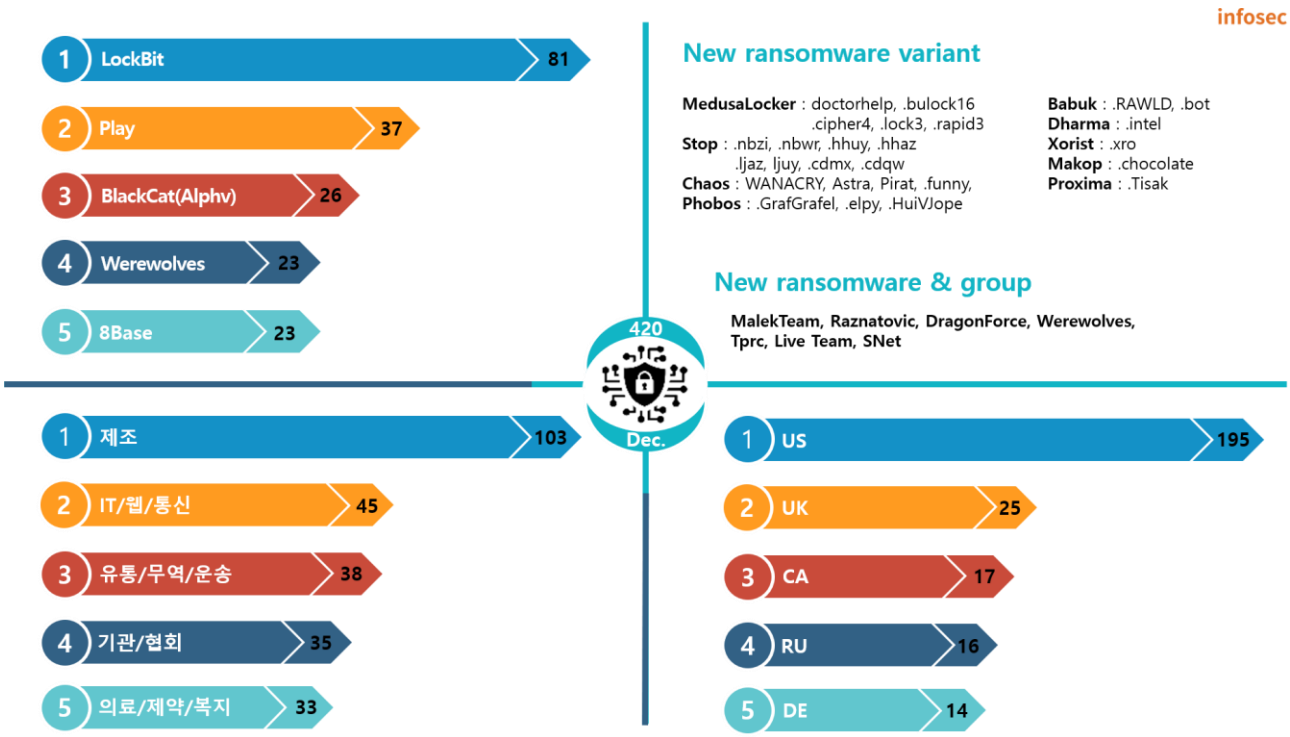


그림 2. 2023 년 12 월 랜섬웨어 위협 현황

새로운 위협

12 월 새롭게 발견된 신규 랜섬웨어 그룹으로는 Malek Team, Raznatovic, DragonForce, Werewolves 가 있다. Malek Team 은 서피스 웹 사이트와 텔레그램 채널을 운영하고 있으며 자신들을 사이버 해킹 분야의 다국적 팀으로 소개하고 있다. 이들은 이스라엘의 병원과 제조업체를 포함한 5 개 조직에 대해 공격을 수행했다는 글을 게시했으며, 이 중 일부는 유출 데이터도 포함된 것으로 확인됐다.

Raznatovic의 경우는 RansomedVC의 계보를 잇는 그룹이다. RansomedVC는 지난 10월에 활동을 개시해 소니(Sony)를 해킹했다고 주장하며 주목받은 랜섬웨어 그룹이다. 이들은 활동 개시 첫 주에만 200 명 이상의 회원을 확보한 이력을 보유하고 있다. 그러나 수사기관의 압박이 시작되자 돌연 랜섬웨어 빌더를 포함한 각종 인프라를 판매한다는 글을 포럼에 게시한 후 6 명이 체포됐으며, 어리고 미숙한 계열사 고용 등의 이유로 사라졌다. 이후, 자신들을 'Ransomed.VC aka Raznatovic'라고 소개하는 그룹이 활동을 개시한 것으로 보아 Raznatovic 가 인프라를 구매한 것으로 추정된다.

Werewolves 그룹은 등장 이후 심상치 않은 움직임을 보이고 있다. 이 그룹이 운영하는 서피스 웹 사이트에는 23 개나 되는 조직의 데이터를 탈취했다고 주장하는 글과 일부 유출 데이터가 게시되었다. 또한 사이트에서는 버그 바운티[6]를 자체적으로 개최하고 있으며 웹 사이트 취약점, 소프트웨어 취약점, Tor 브라우저 취약점 등을 제보하는 자에게 최대 100 만 달러(한화 약 13 억 2000 만원)의 현상금을 지불한다고 명시하고 있다.

Chaos 랜섬웨어의 변종인 Astra 랜섬웨어도 발견됐다. Chaos는 2021년 6월에 처음 발견되어 여러 버전이 출시됐으며, 다크웹 해킹 포럼에 빌더가 공개되어 불특정 다수가 이를 악용한 변종을 대량 생산하기도 했다. 이후 Yashma, Onyx 등 다양한 이름의 랜섬웨어들이 Chaos를 기반으로 등장하여 많은 피해를 발생시키기도 했다. 이번에 발견된 Astra 랜섬웨어도 Chaos 를 기반으로 하고 있다. AES 로 파일을 암호화하고 해당 키를 RSA 로 보호한다는 특징으로 인해 복호화가 어려워 감염 예방에 힘써야 한다.

[6] 버그 바운티 : 기업의 소프트웨어나 시스템의 보안 취약점을 찾는 것에 대해 보상을 지급하는 제도

Top5 랜섬웨어

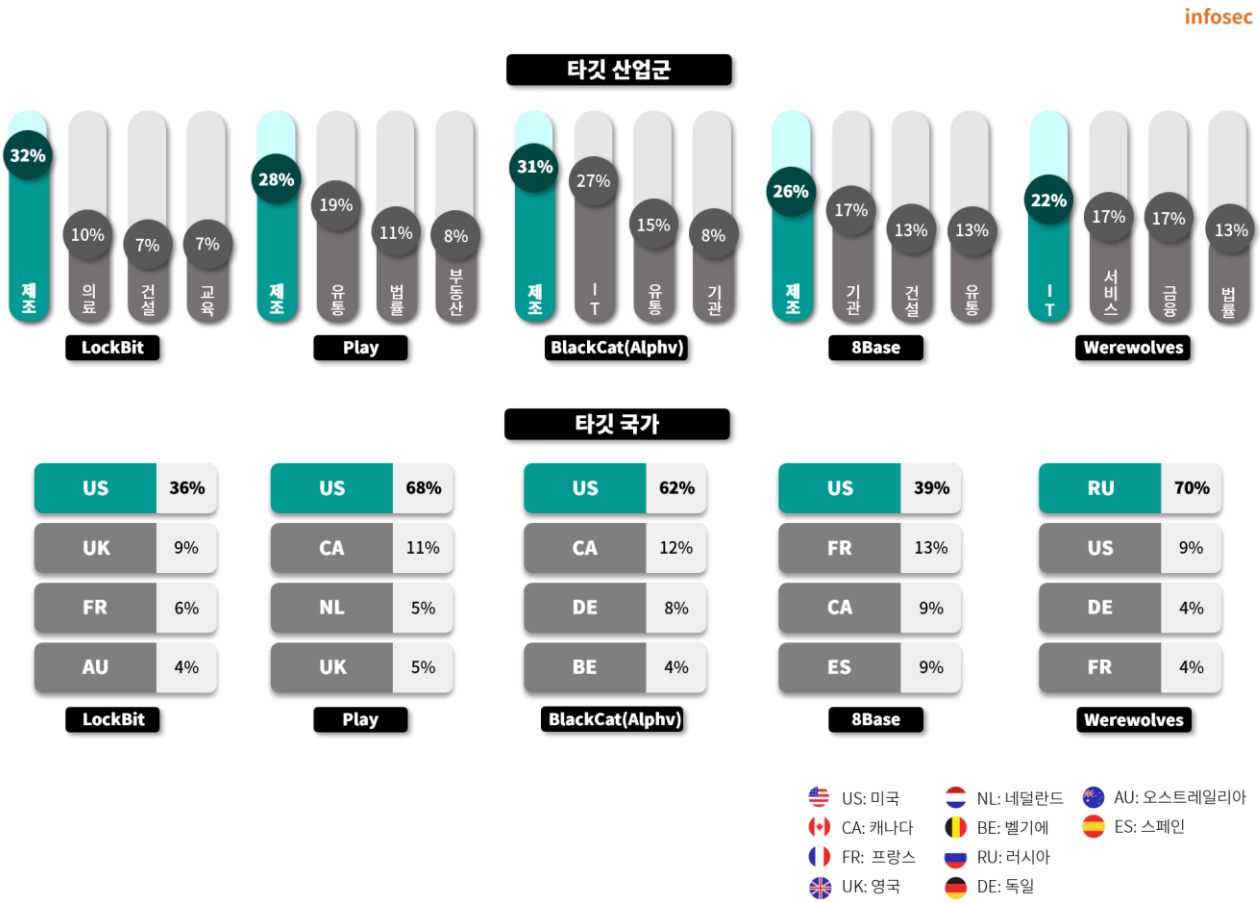


그림 3. 산업/국가별 주요 랜섬웨어 공격 현황

12 월 가장 많은 피해를 발생시킨 랜섬웨어 그룹은 LockBit 이다. LockBit 은 독일 에너지청인 Dena 에 대해 공격을 수행했다고 주장하며, 12 월 26 일까지 협상에 응하지 않을 시 데이터를 유출시키겠다는 협박성 글을 게시하기도 했다. Dena 는 사이버 공격이 있었다는 사실은 인정했지만 랜섬웨어로 인한 공격인지에 대해서는 밝히지 않았다. 또한, LockBit 은 BlackCat(Alphv)이 폐쇄된 것을 기회로 삼아 BlackCat(Alphv)의 개발자 및 계열사에 대해 협업을 제안하기도 했다. 실제로 기존 BlackCat(Alphv) 사이트에 있던 Dena 자료가 LockBit 유출 사이트에도 게시됨에 따라 이적한 계열사가 존재하는 것으로 보인다.

Play 랜섬웨어 그룹은 2022 년 6 월부터 10 월 사이에 전 세계 약 300 개 조직을 공격했으며, 그중 일부는 국가 주요 기반 시설도 포함되어 있어 상당히 큰 영향력을 행사하는 그룹으로 알려져 있다. 이로 인해 최근 FBI 는 미국의 사이버 보안 및 인프라 보안국(CISA) 및 호주 사이버 보안 센터(ACSC)와 함께 Play 에 대해 경고하는 합동 사이버 보안 권고문을 발표하기도 했다.

BlackCat(Alphv)은 국제 수사 기관의 공조로 인해 인프라 폐쇄와 복구를 반복하고 있다. 이들은 FBI 가 인프라를 폐쇄시켰음에도 다시금 인프라를 복구하고 FBI 에 보복하겠다는 선언을 했다. 또한 XSS 포럼에서 BlackCat(Alphv)과 LockBit 은 랜섬웨어 카르텔을 형성해야 한다는 대화를 주고받기도 해 추후 협력 관계가 형성될 수도 있고, 수사 기관의 관심을 돌리기 위해 이전과 같이 리브랜딩 수순을 거칠 가능성도 있다.

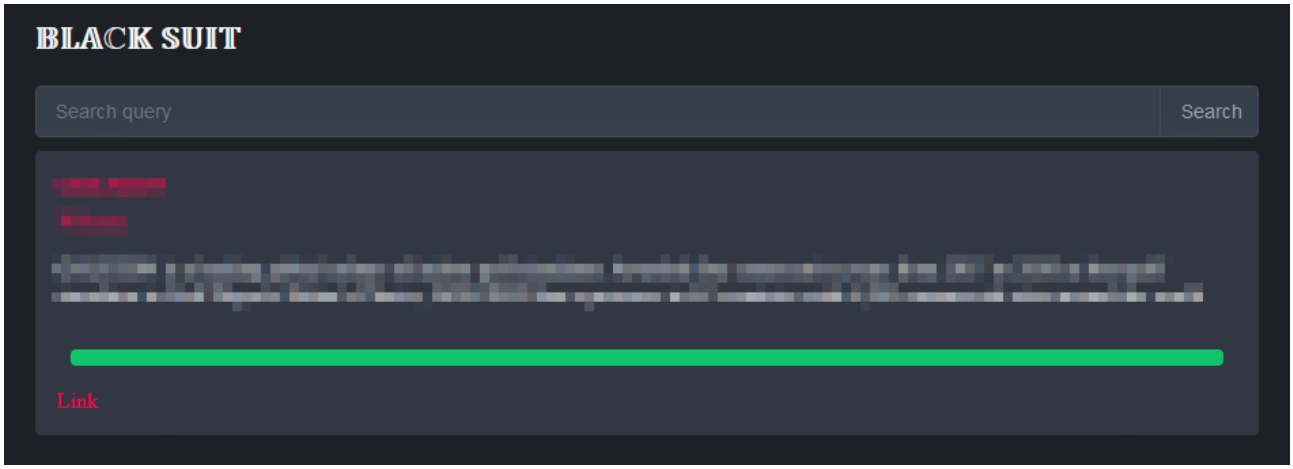
8base 랜섬웨어 그룹은 2023 년 5 월 다크웹 유출 사이트를 개설한 이후 꾸준히 활동을 이어가고 있다. 이들은 Phobos 랜섬웨어의 변종을 활용해 공격을 수행하고 있다. 특히, SmokeLoader[7]를 통해 랜섬웨어를 유포하거나 난독화된 랜섬웨어를 로더 자체에 포함하여 시스템을 감염시킨다. 이처럼 SmokeLoader 는 주로 피싱 메일을 통해 배포되므로 출처가 불분명한 이메일의 첨부파일은 가급적 다운로드를 지양하여 감염을 예방할 것을 권장한다.

Werewolves 는 12 월에 새롭게 발견된 랜섬웨어 그룹이다. 이들은 LockBit 3.0 랜섬웨어와 유출된 Conti 의 해킹 도구들을 사용해 취약한 공공 서비스를 대상으로 공격을 수행하고 있다. 이들로 인해 23 개의 조직이 수백 테라바이트의 데이터를 탈취당하는 피해를 입었다. 그중 16 개 기업은 러시아를 대상으로 수행된 공격이다. 또한 LockBit 3.0 을 사용하는 점과 LockBit 에서 게시한 피해 조직과 6 건이 겹치는 등 LockBit 과의 연관성이 제기되고 있다.

[7] SmokeLoader : 감염된 시스템에 다른 악성코드를 다운로드하는 데 사용되는 악성코드

■ 랜섬웨어 집중 포커스

BlackSuit 랜섬웨어 개요



출처: BlackSuit 랜섬웨어 그룹 다크웹 유출 사이트

BlackSuit는 2023년 5월 등장했으며, Royal 이 리브랜딩한 랜섬웨어 그룹이다. 이들은 Windows와 Linux 를 모두 타깃으로 공격해 몸값을 요구하는 동시에 데이터를 유출하겠다고 협박하는 이중 협박 방식을 취하고 있다.

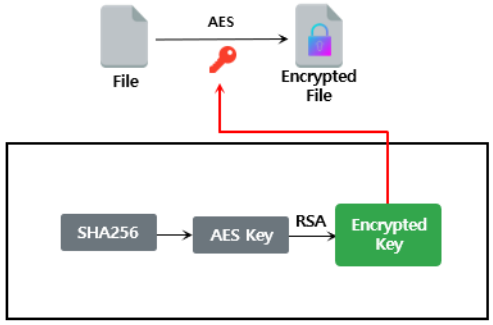
BlackSuit 의 전신인 Royal 은 2022 년 6 월에 활동을 종료한 Conti 랜섬웨어가 해체되고 난 뒤에 파생된 랜섬웨어 그룹이다. 등장 이래로 350 개가 넘는 조직에 대해 협박을 통해 2 억 7,500 만 달러(한화 약 3,627 억 원) 상당의 금액을 요구한 것으로 밝혀졌으며, 다크웹 유출 사이트에 데이터가 게시된 조직만 해도 200 개의 업체를 상회한다. 이렇듯 상당한 영향력을 보여주던 Royal 은 2023 년 5 월 미국 댈러스 시를 공격한 뒤로 수사기관의 압박이 거세지자 7 월경부터 잠잠한 모습을 보이더니 결국 10 월에 자취를 감춘 채 BlackSuit로 완전히 리브랜딩을 완료했다.

BlackSuit 는 피싱 메일의 첨부파일, 토렌트 웹 사이트, 악성 광고 등을 통해 전파되고 있으며, 최근 국내 A기업의 유출 데이터를 공개하는 사건이 발생했다. A기업은 랜섬웨어 공격이 발생한지 3주가 지나서야 고객에게 피해 사실을 고지하고 일부 고객의 개인정보가 유출된 사실을 밝혔다. 또한, 랜섬웨어 공격 이후 일부 사용자는 A 기업을 사칭한 피싱 문자를 받는 등의 피해를 입기도 했다. 이처럼 유출된 개인정보를 통해 피싱이나 스미싱 등의 2 차 피해가 발생할 수 있어 각별히 주의가 필요하다.

BlackSuit Ransomware

암호화 키

AES-256-CBC 알고리즘으로 파일 암호화를 하고, 해당 키를 RSA로 보호



암호화 방식

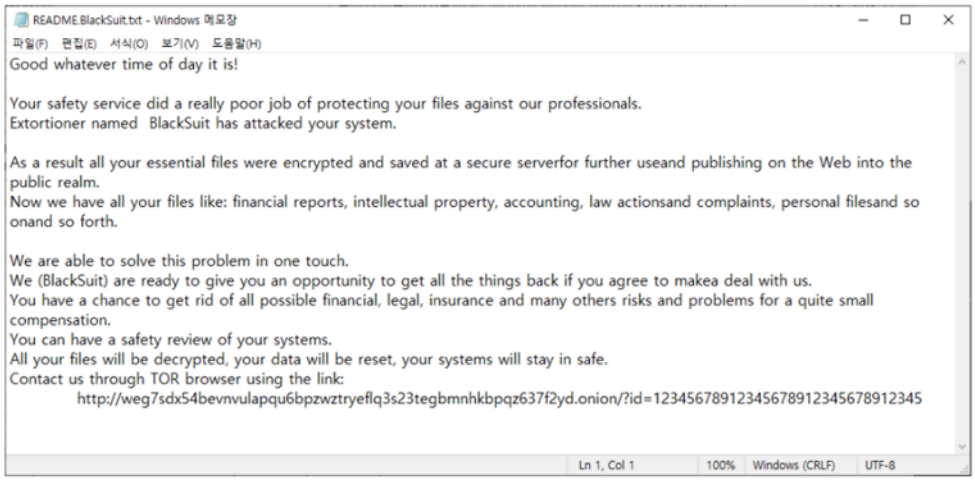
파일 크기 256KB 이상 : 파일 크기의 약 10% 간격으로 간헐적 암호화

파일 크기 256KB 미만 : 파일 전체 암호화

특징

- 인자전달
- 시스템 복구 옵션 제거
- 부분 암호화
- AES & RSA 암호화
- Royal 리브랜딩
- 멀티쓰레드

랜섬노트


README.BlackSuit.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

Good whatever time of day it is!

Your safety service did a really poor job of protecting your files against our professionals.
Extortioner named BlackSuit has attacked your system.

As a result all your essential files were encrypted and saved at a secure serverfor further useand publishing on the Web into the public realm.
Now we have all your files like: financial reports, intellectual property, accounting, law actionsand complaints, personal filesand so onand so forth.

We are able to solve this problem in one touch.
We (BlackSuit) are ready to give you an opportunity to get all the things back if you agree to makea deal with us.
You have a chance to get rid of all possible financial, legal, insurance and many others risks and problems for a quite small compensation.
You can have a safety review of your systems.
All your files will be decrypted, your data will be reset, your systems will stay in safe.
Contact us through TOR browser using the link:
http://weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd.onion/?id=12345678912345678912345678912345

Ln 1, Col 1 100% Windows (CRLF) UTF-8

README.BlackSuit.txt

변경 확장자

.BlackSuit

제작 언어

C/C++

그림 4. BlackSuit 랜섬웨어 개요

BlackSuit 랜섬웨어 전략

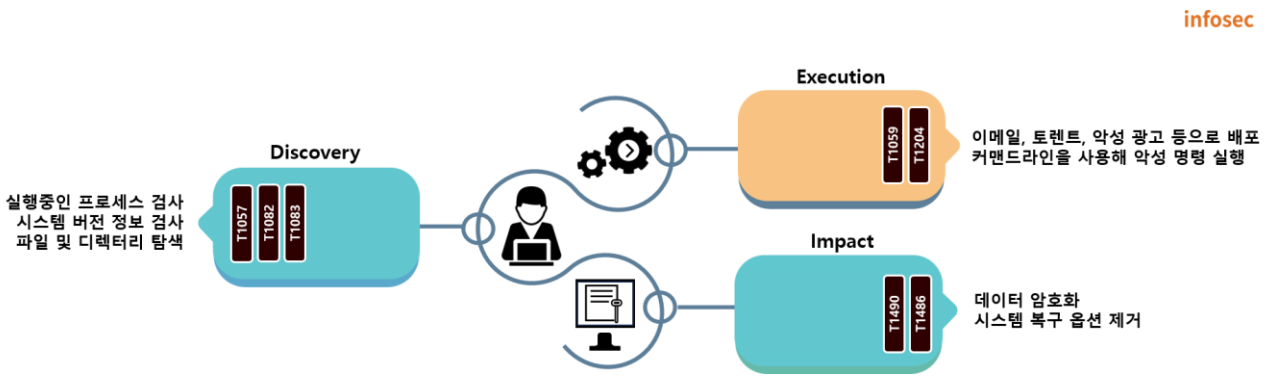


그림 5. BlackSuit 랜섬웨어 공격 전략

BlackSuit 랜섬웨어는 첨부파일에 랜섬웨어를 첨부하거나 랜섬웨어가 실행되게 하는 매크로를 포함한 문서 파일을 첨부해 파일 실행 시 사용자도 모르게 감염되게 하는 공격을 진행한다. 또한, 악성 광고 등 클릭과 동시에 자동으로 랜섬웨어가 설치되는 사이트로 리다이렉트 되거나 다운로더 형태의 악성코드를 통해 설치되기도 해 주의가 필요하다.

해당 랜섬웨어는 다양한 인자 전달을 통해 공격자가 편의를 도모한 것으로 보이며, 특정 인자가 전달되지 않으면 암호화가 진행되지 않고 즉시 프로세스가 종료되도록 설계돼 있다. 이는 탐지 우회 및 분석 방해의 효과를 노린 것으로 분석된다.

인자	설명
-p {target path}	지정된 경로의 내용만 암호화
-name {32byte string}	고유 ID, 전달되지 않을 경우 프로세스 종료
-percent {0~100}	암호화 강도 지정
-list {text files}	암호화 할 대상이 작성된 텍스트 파일
-delete	자가 삭제
-network	네트워크 공유 자원 암호화
-local	로컬 시스템 암호화
-disablesafeboot	안전 모드 부팅 비활성화
-noprotect	뮤텍스 생성 비활성화

표 1. BlackSuit 랜섬웨어 인자

BlackSuit 의 인자 중, 특히 주목해야 할 인자는 -name 과 -percent 다. 매크로나 스크립트를 통해 랜섬웨어가 실행될 때 -name 인자와 함께 전달되는 32byte 의 문자열은 피해자의 고유 ID 로 사용되며 랜섬노트에도 기재된다. 만약 해당 인자가 전달되지 않을 경우 프로세스가 종료되며, 해당 인자 값은 단순히 피해자를 식별하기 위한 값으로 사용되어 32byte 문자열 형태만 전달되면 랜섬웨어 실행이 가능하다.

-percent 인자와 함께 전달되는 인수를 통해서 암호화 강도를 지정할 수 있는데, 256KB 이상의 파일에 대해서 간헐적인 암호화 방식을 채택한 BlackSuit 는 -percent 인자가 전달되지 않을 경우에는 기본적으로 100 이 전달된 것으로 간주하여 파일 크기의 약 10% 단위로 간헐적 암호화를 진행한다.

$$N = \left(\frac{X}{10}\right) \times \left(\frac{\text{Original File Size}}{100}\right)$$

[BlackSuit 암호화 강도 계산식]

- N : 간헐적 암호화에 사용될 바이트 수
- X : -percent 인자와 함께 전달되는 인수의 값
- 계산된 N 은 최종적으로 16 의 배수로 값을 내림

BlackSuit 는 커맨드 라인 명령 실행을 통해 VSC(Volume Shadow Copy)[8]를 Quiet 옵션으로 피해자 모르게 삭제해 사용자가 임의로 복구할 수 없도록 막는다. 이를 통해 안전 모드로 부팅해 피해자가 복구 옵션을 사용하는 것을 막기 위해 safeboot 옵션을 제거한다. 이 랜섬웨어는 32Bit 프로그램이지만, 64Bit 의 경우에도 VSC 를 통한 복구를 막기 위해 64Bit 에 해당하는 명령어도 함께 실행시키는 용의주도함을 보이고 있다. 이러한 명령들이 실행되고 나면 그 즉시 컴퓨터가 재부팅 되어 사용자가 어떠한 조치도 취할 수 없이 랜섬웨어에 속수무책으로 당하게 된다.

[8] VSC : Windows 시스템에서 파일이나 폴더의 백업 사본을 생성하고 유지하는 기능

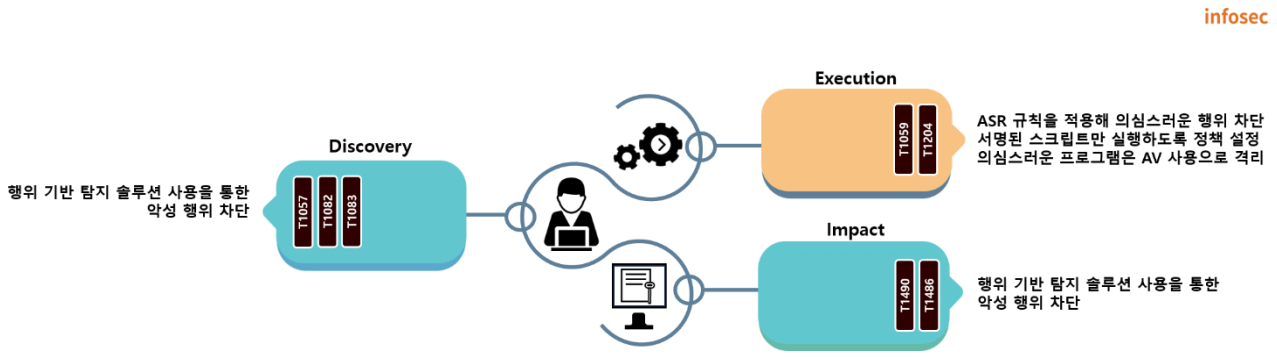


그림 6. BlackSuit 랜섬웨어 대응방안

BlackSuit 랜섬웨어의 행위들은 대부분 시스템의 기본 기능을 악용하므로 시그니처 기반의 보안 솔루션에서는 정확한 구분이 어려울 수 있다. 이러한 문제를 해결하기 위해 행위 기반으로 탐지하는 보안 솔루션을 사용하거나 ASR(Attack Surface Reduction)[9] 규칙을 활성화시킨다면 시스템 기본 기능이지만 비정상적으로 발생한 부분에 대해서 차단할 수 있다.

이러한 케이스의 랜섬웨어는 무엇보다 사전에 감염을 방지하기 위해 힘써야 한다. 다양한 경로로 감염될 수 있는 만큼 조직에서는 구성원들의 보안 인식 제고를 위한 교육을 진행하는 등의 방법이 필요하다.

특히, 출처를 알 수 없는 이메일의 첨부파일을 다운로드하거나 열어보는 행위, 애플리케이션의 공식 홈페이지가 아닌 곳에서 다운로드하거나 업데이트를 수행하는 행위, 취약한 웹 사이트의 광고 배너를 클릭하는 등의 행위 등은 조심해야 한다. 개인 혹은 조직에서 보안 인식 제고를 위해 구성원들에게 이러한 행동을 자제할 것을 권고한다면 랜섬웨어의 감염 가능성을 최소화할 수 있을 것이다.

[9] ASR : 악성코드의 공격 경로를 차단하는 기법

Indicator Of Compromise

BlackSuit : SHA256

90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c
1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e
449df90b819d01d290d218929bd33ee24941b3e6c00cdedc0e6f2714aea8460b
feced22ef920c40e032e12b9eb315591a7b6adcd371453c7d2fa08e2c8972aac

File Name

sys32.exe

■ 참고 사이트

URL : https://www.bleepingcomputer.com/news/security/fbi-alphv-ransomware-raked-in-300-million-from-over-1-000-victims/

URL : https://www.bleepingcomputer.com/news/security/how-the-fbi-seized-blackcat-alphv-ransomwares-servers/

URL : https://techcrunch.com/2023/11/15/cisa-fbi-royal-ransomware-blacksuit-sanctions/

URL : https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/

URL : https://www.resecurity.com/blog/article/Exposing-Cyber-Extortion-Trinity-BianLian-White-Rabbit-Mario-Ransomware-Gangs-Spotted-Joint-Campaign

URL : https://thecyberexpress.com/werewolves-ransomware-group/

URL : https://www.scmp.com/tech/tech-trends/article/3246612/chatgpt-aided-ransomware-china-results-four-arrests-ai-raises-cybersecurity-concerns

URL : https://www.bleepingcomputer.com/news/security/fake-f5-big-ip-zero-day-warning-emails-push-data-wipers/

ownCloud 정보 노출 및 인증 우회 취약점(CVE-2023-49103/ CVE-2023-49105)

■ 취약점 개요

2023 년 11 월, 파일 공유 및 관리를 위한 오픈소스 소프트웨어 ownCloud 에서 정보 노출 취약점(CVE-2023-49103)과 인증 우회 취약점(CVE-2023-49105)이 발견됐다. ownCloud 는 비용 없이 개인 서버에 구축이 가능한 파일 호스팅 서비스로 드롭박스(DropBox), 구글 드라이브(Google Drive)와 같은 상용 클라우드 스토리지 서비스를 대체할 수 있어 개인 및 기업에서 널리 사용되고 있다. 특히 아마존 웹 서비스(AWS)와 애저(Azure) 등 다른 클라우드 플랫폼에 ownCloud 호스팅 서버를 구축하거나 스토리지를 연결하여 사용하는 경우, 해당 취약점들을 악용한 2 차 피해의 위험이 있어 각별한 주의가 필요하다.

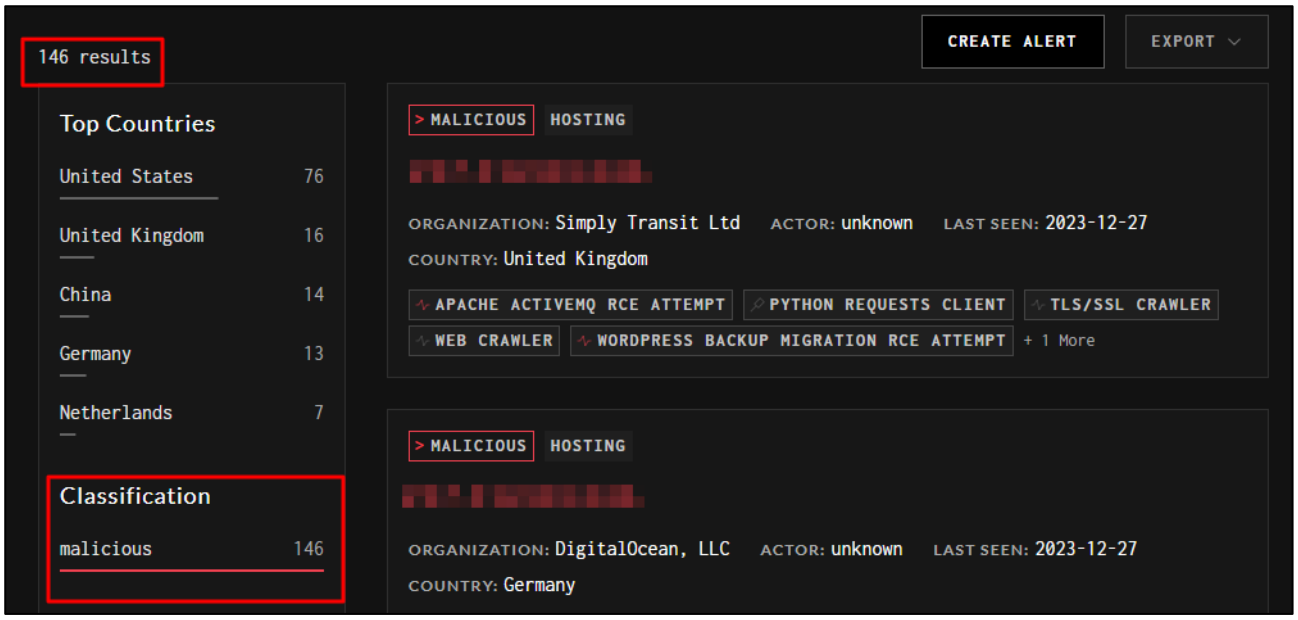
먼저, 정보 노출 취약점(CVE-2023-49103)은 취약한 graphapi[10] 사용과 미흡한 검증으로 인해 발생한 취약점이다. 악의적인 공격자는 phpinfo 에 액세스하여 자격증명, 서버 라이선스 키, 관리자 계정 등 서버 측의 민감 데이터에 접근할 수 있다. 해당 취약점은 CVSS 10.0 으로 평가되어 매우 높은 위험도를 가지고 있다.

인증 우회 취약점(CVE-2023-49105)은 ownCloud core 의 취약한 인증 프로세스 구현으로 인해 발생하는 취약점이다. 이 취약점을 악용하면 인증되지 않은 공격자가 서버 내 모든 파일에 대한 액세스 권한을 획득할 수 있으며, 이를 통해 권한 상승과 원격 코드 실행이 가능해져 서버를 장악할 수 있다. 해당 취약점은 CVSS 9.8 로 평가되어 높은 위험도를 가지고 있다.

2023 년 11 월 25 일에 Proof of Concept(PoC)가 공개된 이후, ownCloud 를 대상으로 대량의 익스플로잇[11] 시도가 확인되고 있다. 따라서 ownCloud 사용자들은 반드시 취약점에 대한 보안 업데이트를 적용하고, 취약한 버전을 사용 중이라면 해당 취약성을 조사하고 대응하는 조치를 취해야 한다.

[10] graphapi : Microsoft Graph API 기반의 ownCloud Server 확장 프로그램

[11] 익스플로잇(Exploit) : 보안 취약점을 이용한 공격



출처: GreyNoise

그림 1. 익스플로잇 시도 (출처 - GREYNOISE)

특히 23 년 상반기부터 MOVEit[12], GoAnywhere[13] 등 파일 공유 소프트웨어 취약점을 악용한 랜섬웨어 그룹의 대규모 공격이 발생하고 있는 만큼, 취약한 버전의 ownCloud 를 사용하고 있는 개인 및 기업은 보안 패치를 적용해야 한다.

■ 영향받는 소프트웨어 버전

CVE-2023-49103 취약점에 영향을 받는 ownCloud 의 버전은 다음과 같다.

S/W 구분	취약 버전
ownCloud	graphapi 0.2.0 ~ 0.3.0 버전의 ownCloud Docker (2023 년 2 월 이후 Docker 이미지)

※ 도커로 구성하지 않은 환경이라도 취약한 graphapi 를 설치한 경우 취약점이 발생한다.

CVE-2023-49105 취약점에 영향을 받는 ownCloud 의 버전은 다음과 같다.

S/W 구분	취약 버전
ownCloud	10.6.0 ~ 10.13.0

[12] MOVEit : Progress Software 에서 개발한 기업용 파일 전송 소프트웨어

[13] GoAnywhere : Fortra 에서 개발한 파일 전송 솔루션

■ 공격 시나리오

ownCloud 취약점(CVE-2023-49103, CVE-2023-49105)을 이용한 공격 시나리오는 다음과 같다.

정보 노출 취약점(CVE-2023-49103) 공격 시나리오

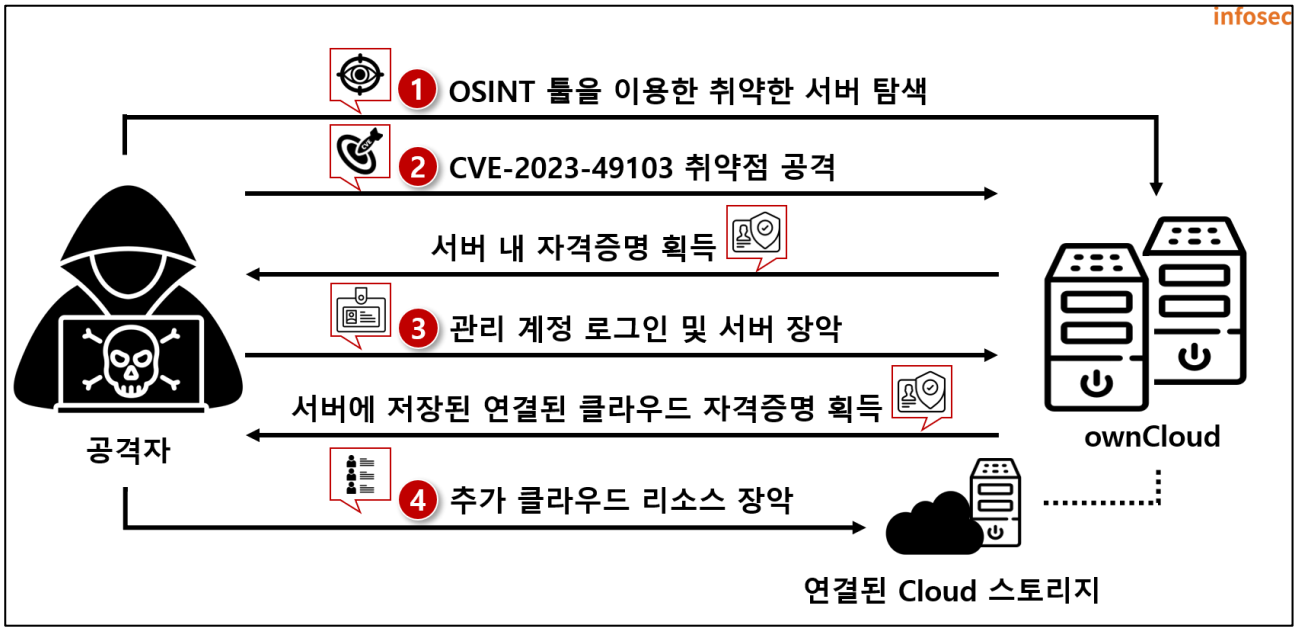


그림 2. CVE-2023-49103 공격 시나리오

① 공격자가 shodan과 같은 OSINT[14] 툴을 이용하여 취약한 ownCloud 서버 탐색
② CVE-2023-49103 취약점을 이용하여 서버의 phpinfo 파일 접근 후 자격증명 획득
③ 획득한 자격증명을 이용하여 ownCloud 서버 로그인 및 서버 장악
④ 공격자가 서버 내 저장되어 있는 연결된 다른 클라우드의 자격증명 획득
⑤ 획득한 자격증명을 이용하여 연결된 다른 클라우드 리소스 장악

[14] OSINT(Open Source Intelligence): 오픈소스를 이용하여 수집한 외부에 공개된 정보

인증 우회 취약점(CVE-2023-49105) 공격 시나리오

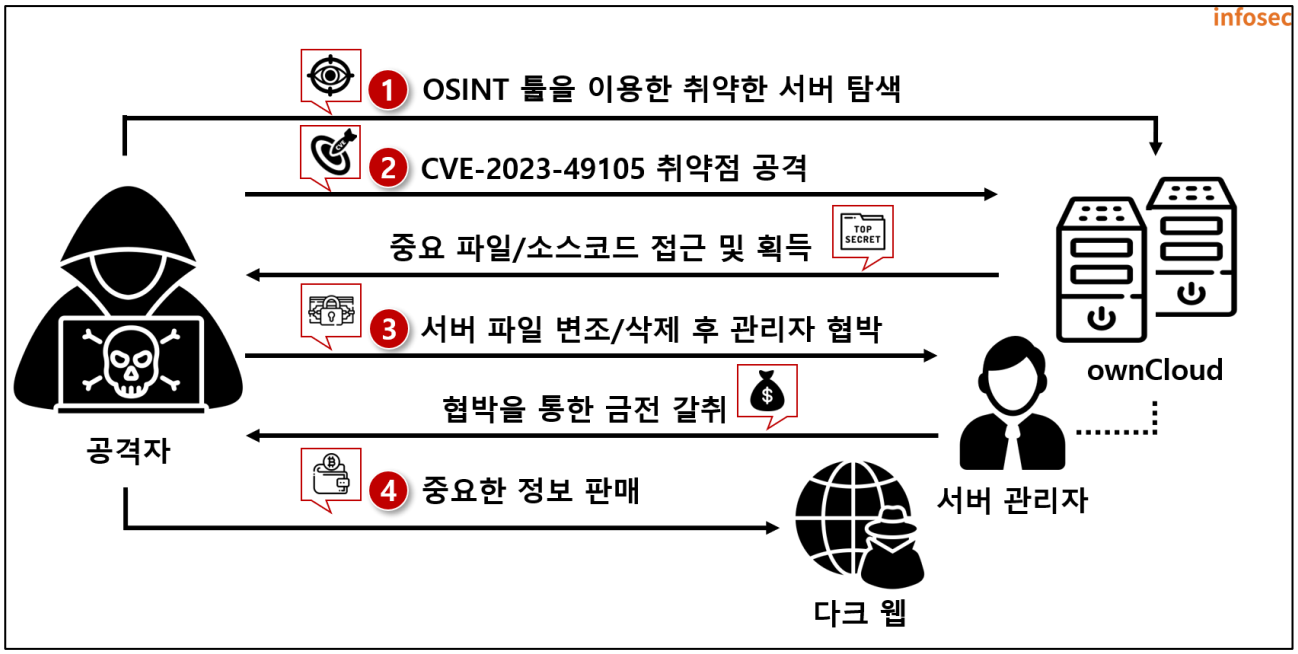


그림 3. CVE-2023-49105 공격 시나리오

① 공격자가 shodan과 같은 OSINT 툴을 이용하여 취약한 ownCloud 서버 탐색
② CVE-2023-49105 취약점을 이용하여 서버 내 중요 파일 및 소스코드 접근
③ 서버 내 파일 변조 및 삭제 후 파일 복구를 빌미로 관리자 협박 및 금전 갈취
④ 또한, 서버에서 획득한 중요 정보를 다크웹에 판매한 후 금전 획득

■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2023-49103 과 CVE-2023-49105 의 동작 과정을 살펴본다.

이름	정보
피해자	Ubuntu-22.04.1 도커 이미지: ownCloud/server 10.12.1
공격자	Ubuntu-22.04.1

※ 해당 취약점 테스트 시, AWS 기반의 클라우드로 연결되어 IAM 정보가 포함되어 있다고 가정한다.

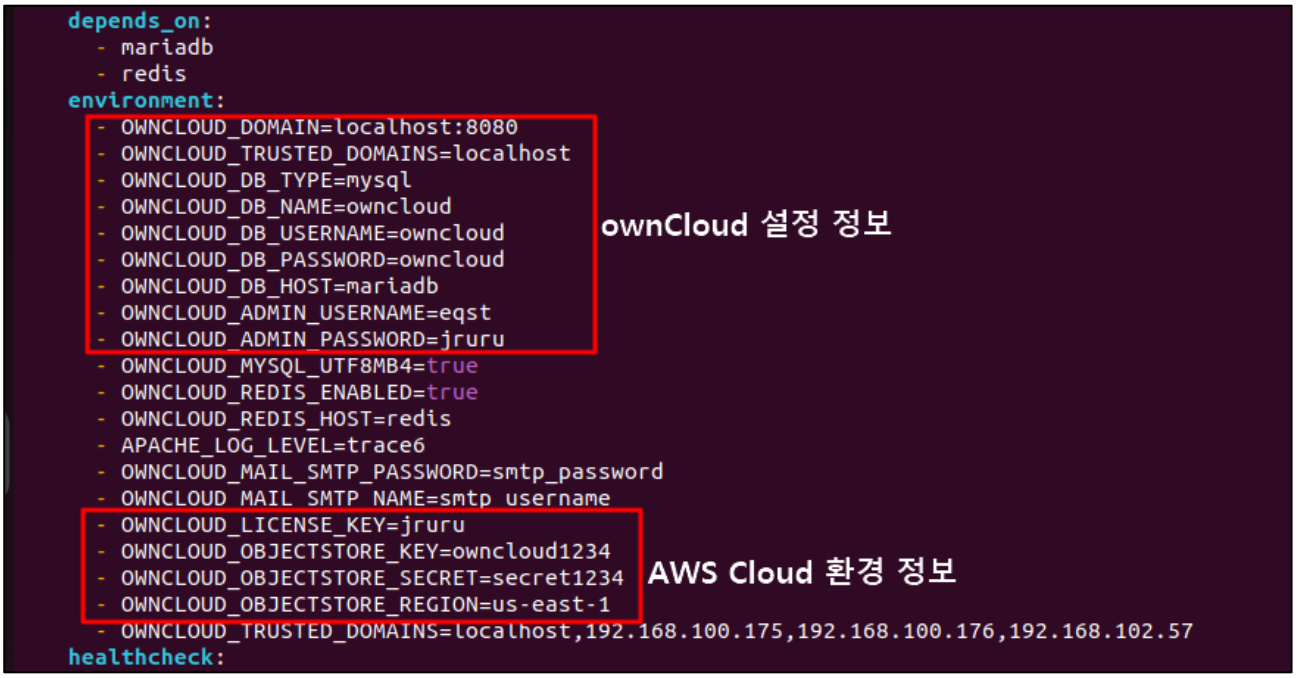


그림 4. ownCloud docker 정보

■ 취약점 테스트

- ownCloud 정보 노출 취약점(CVE-2023-49103)

Step 1) 피해자는 ownCloud 공식 사이트에서 제공하는 docker 설치 방법을 기반으로 취약한 버전의 ownCloud 서버를 구축한다.

- ownCloud docker 설치: https://doc.owncloud.com/server/next/admin_manual/installation/docker/

명령어	$ docker-compose up -d -d 옵션: detach 모드로 백그라운드로 docker 를 실행시키는 옵션

※ 이때, OWNCLOUD_TRUSTED_DOMAINS 에 공격자의 주소를 추가해야 한다. 해당 설정 값은 접속 허용 IP 이며, 해당 값이 안전하게 설정되어 있을 경우 외부에서 접근이 불가하여 해당 취약점 악용이 불가하다.

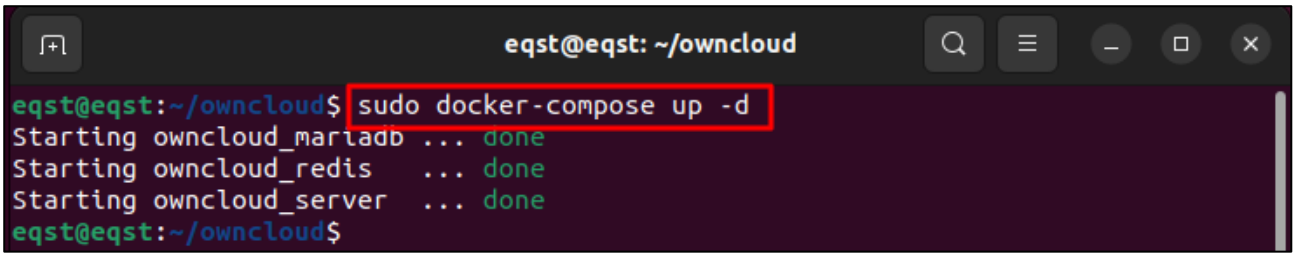


그림 5. ownCloud 서버 구현

Step 2) 공격자는 아래의 명령어를 통해 민감 정보 중 하나인 관리자 계정을 획득할 수 있다.

- PoC 코드: https://github.com/api0cradle/CVE-2023-23397-POC-Powershell

명령어	**- 구문 예시**
	$ curl -i 'http://**[피해자 서버]**/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/**[확장자]**' | grep **[검색할 문자열]**
	
	- 페이로드 (192.168.100.176:8080 ownCloud 서버에서 ADMIN 검색)
	$ curl -i 'http://**192.168.100.176:8080**/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php/.**css**' | grep **ADMIN**
	※ -i 옵션: 헤더 정보를 출력하는 명령어

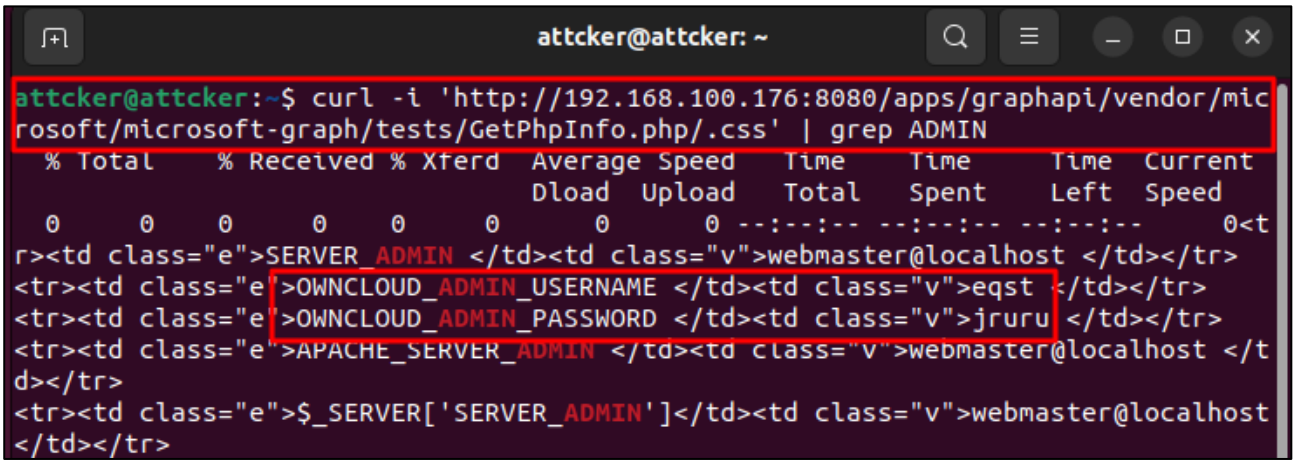


그림 6. 공격 페이로드 결과

페이로드에 입력 가능한 확장자 리스트는 아래와 같으며, 해당 확장자들은 액세스 제어 우회를 위해 사용된다. 자세한 내용은 뒷장의 취약점 상세 분석에서 확인할 수 있다.

우회 가능한 확장자				
.css	.js	.svg	.gif	.png
.html	.woff	.ico	.jpg	.jpeg
.json	.properties	.min.map	.js.map	.auto.map

- ownCloud 인증 우회 취약점(CVE-2023-49105)

Step 1) 공격자는 PoC 가 저장된 git 파일을 복사한 뒤, 피해자 ownCloud 서버 주소와 사용자 ID 를 이용하여 페이로드를 작성한다. 페이로드 실행 시, 접근 가능한 WebDAV 접속 주소를 확인할 수 있다.

- PoC 코드: https://github.com/ambionics/owncloud-exploits

명령어	$ git clone https://github.com/ambionics/owncloud-exploits
	공격 구문 예시는 아래와 같다.
	$ python3 pwncloud-webdav.py http://**[공격자 서버:포트] [ID 정보]**
	$ python3 pwncloud-webdav.py http://192.168.100.176:8080 eqst

※ 이때, OWNCLOUD_TRUSTED_DOMAINS 에 공격자의 주소를 추가해야 한다. 해당 설정 값은 접속 허용 IP 이며, 해당 값이 안전하게 설정되어 있을 경우 외부에서 접근이 불가하여 해당 취약점 악용이 불가하다.

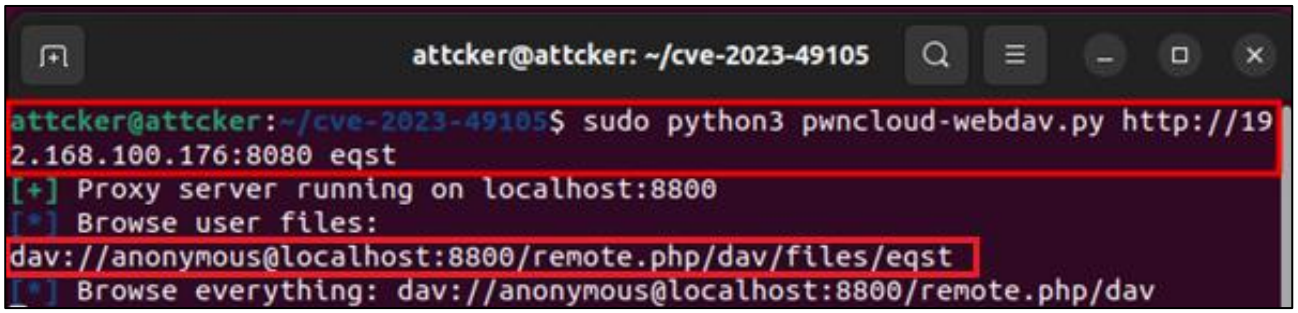


그림 7. PoC 를 통한 공격 시도

Step 2) 확인한 주소를 통해 별도의 인증 없이 WebDAV 서버 접속이 가능하며, 접근한 WebDAV 서버에서 민감 정보가 포함된 파일 읽기/수정/삭제/생성 등 파일에 대한 접근 제어가 가능하다.

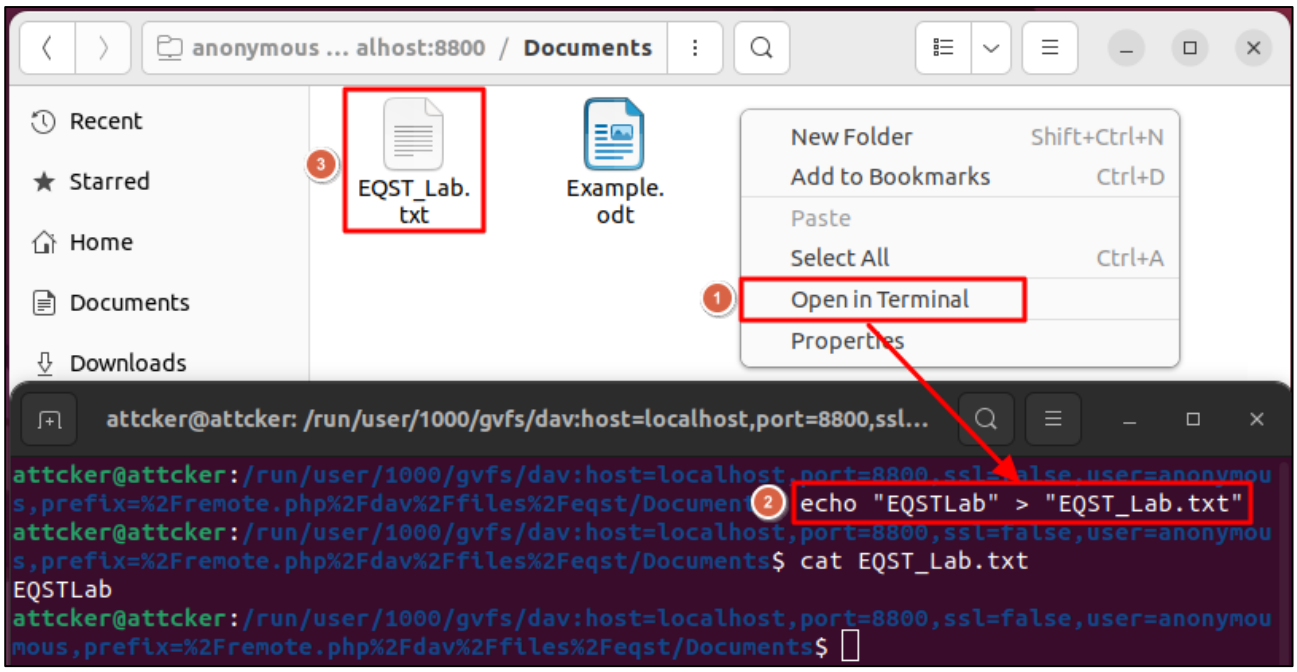


그림 8. 인증 우회를 통한 파일 생성

■ 취약점 상세 분석

- 정보 노출 취약점(CVE-2023-49103)

정보 노출 취약점(CVE-2023-49103)은 docker 파일로 제공하는 ownCloud 의 default 확장 프로그램인 Graph API(graphapi)로 인해 발생하는 취약점이다. graphapi 는 phpinfo() 함수를 통해 환경 변수를 포함한 PHP 구성 정보를 출력하는 외부 라이브러리인 “GetPhpInfo”를 사용한다. GetPhpInfo 는 graphapi 의 엔드포인트로서 인증되지 않은 사용자가 외부에서 직접 접근이 불가능하도록 설계해야 한다. 하지만 취약한 버전의 ownCloud 를 사용할 경우, 엔드포인트 접근 인증 로직이 미흡하여 인증되지 않은 공격자가 외부에서 GetPhpInfo 에 직접 접근하여 민감 정보를 획득할 수 있다. 특히 Docker 를 이용하여 ownCloud 를 구축할 경우, 환경 변수를 통해 관리자 자격 증명 정보, 클라우드와 IAM 정보와 같은 민감 데이터가 포함된 상태로 구성되므로 각별한 주의가 필요하다.

먼저, 취약점 확인을 위해 GetPhpInfo.php 에 직접 접근을 시도해보면, 302 응답 코드(Temporarily Moved)를 반환하며 로그인 페이지인 index.php 로 자동으로 리디렉션하여 접근이 불가능하다.

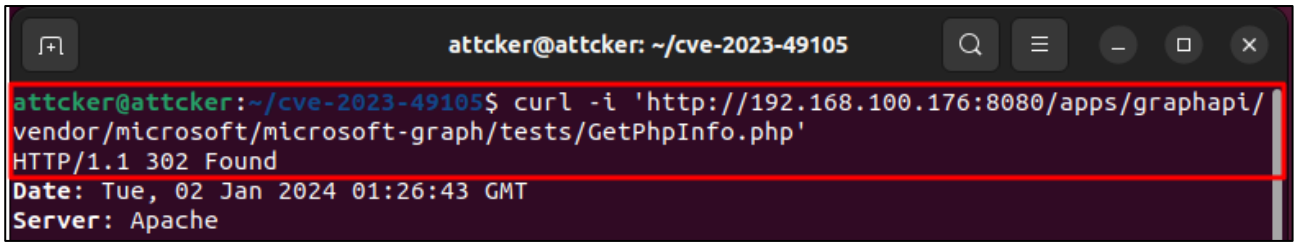


그림 9. GetPhpInfo.php 직접 접근 예시

이는 ownCloud 의 .htaccess 파일 설정을 통한 액세스 제어가 구현되어 있기 때문이다. .htaccess 파일을 확인해보면 mod_rewrite[15] 모듈을 통해 조건과 일치하지 않은 모든 요청은 302 응답을 반환한 뒤, index.php 페이지로 리디렉션 하도록 정의되어 있다.

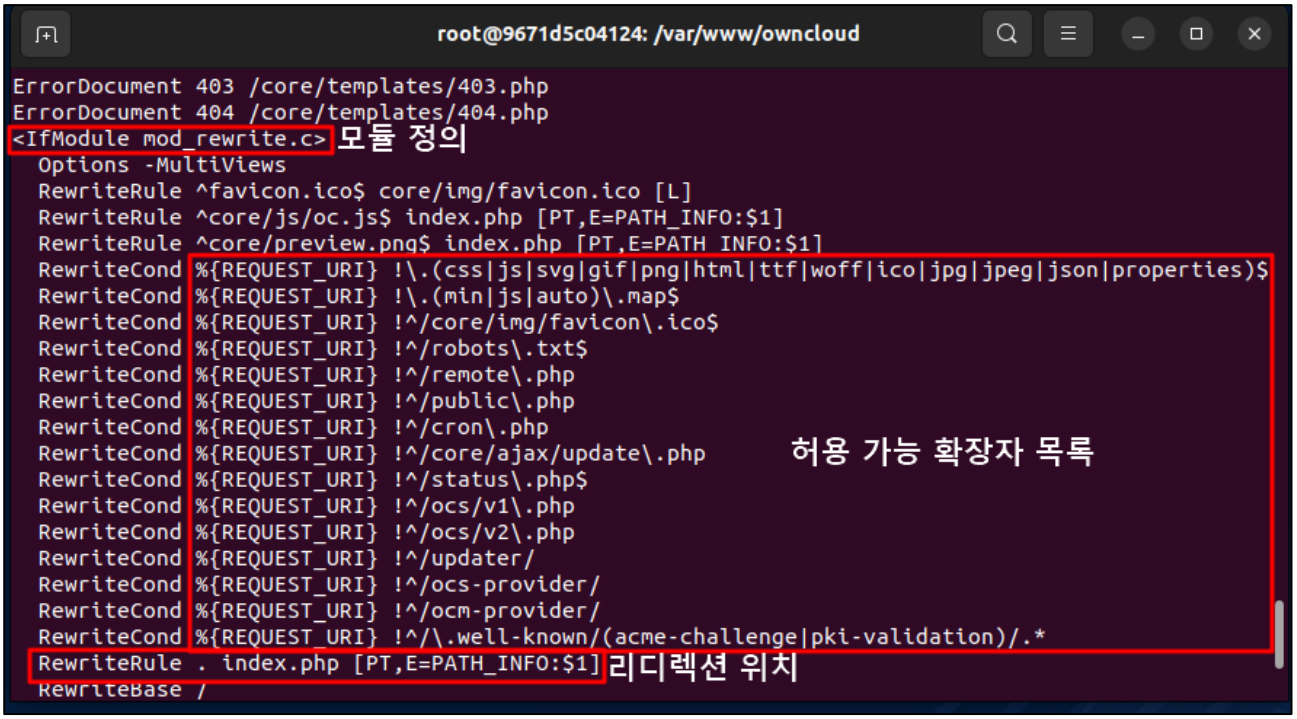


그림 10. .htaccess 파일 내의 mod_rewrite 모듈

[15] mod_rewrite : 서버 Request 를 정해진 Rule 에 의해 다른 URL 또는 File 로 리디렉션 하는 모듈

아래에 정리된 확장자는 mod_rewrite 의 조건에 해당되지 않는 확장자로 .htacess 를 통한 액세스 제어를 우회하기 위한 방법으로 사용한다.

우회 가능한 확장자	설명
.css	CSS(Cascading Style Sheets)는 HTML 요소가 화면에 표시되는 방식을 정의한 파일 형식이다.
.js	웹 페이지에서 실행하기 위한 JS(JavaScript) 코드를 포함하는 파일 형식이다.
.svg	SVG(Scalar Vector Graphics)는 이미지 모양을 설명하기 위한 XML 기반 텍스트 파일 형식이다.
.gif	GIF(Graphics Interchange Format)는 수많은 이미지 또는 프레임을 단일 파일로 결합한 애니메이션 클립 또는 짧은 비디오 파일 형식이다.
.png	PNG(Portable Network Graphic)는 무손실 데이터 압축을 지원하여 웹에서 그래픽을 표현하는 이미지 파일 형식이다.
.html	HTML(Hypertext Markup Language)은 웹 페이지와 그 내용을 구조화하기 위해 사용하는 파일 형식이다.
.woff	woff 인 파일은 WOFF(Web Open Font Format)를 기반으로 하는 웹 글꼴 파일 형식이다.
.ico	응용 프로그램을 나타내는 아이콘으로 사용되는 이미지 파일 형식이다.
.jpg **.jpeg**	JPEG(Joint Photographic Experts Group)의 약자로, 디지털 이미지를 위한 파일 형식이다.
.json	JSON(JavaScript Object Notation)은 사람이 읽을 수 있는 텍스트를 사용하여 데이터를 저장하고 전송하는 데이터 공유를 위한 표준 파일 형식이다.
.properties	properties 는 응용 프로그램의 구성 가능한 파라미터들을 저장하기 위해 자바 관련 기술을 주로 사용하는 파일 형식이다.
.min.map **.js.map** **.auto.map**	Application 빌드 시 생성되는 map 파일은 빌드 된 실행파일이 메모리에 로드 되었을 때, 전역변수, 함수가 위치할 Address 를 기록해 놓은 파일 형식이다.

따라서 해당 확장자들을 포함하여 GetPhpInfo.php 를 직접 접근 요청하면 액세스 제어 규칙을 우회해 민감정보에 접근할 수 있다.

ex) /apps/graphapi/vendor/microsoft/microsoft/graph/tests/GetPhpInfo.php/.css

ex) /apps/graphapi/vendor/microsoft/microsoft/graph/tests/GetPhpInfo.php/.png

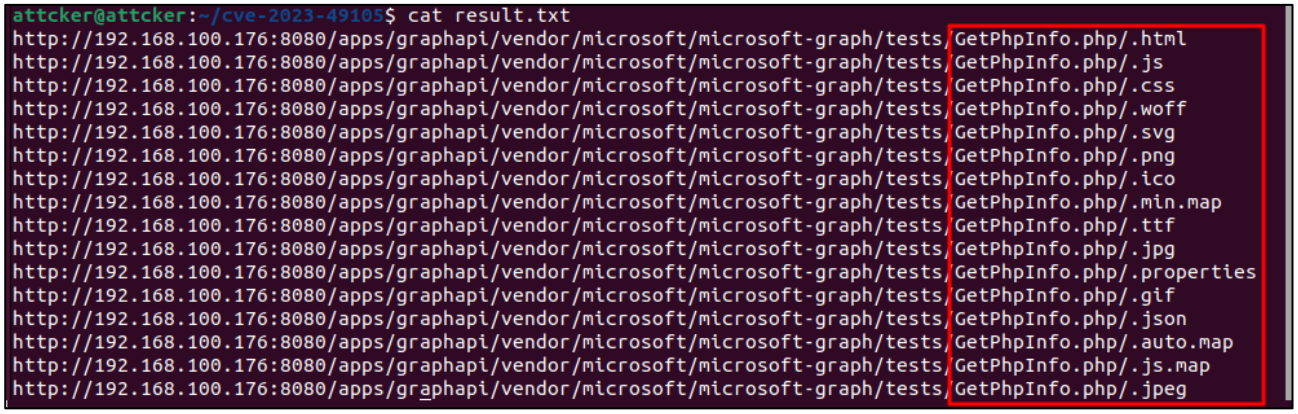


그림 11. 확장자를 통한 액세스 제어 규칙 우회

- 인증 우회 취약점(CVE-2023-49105)

CVE-2023-49105 취약점은 ownCloud core 의 미흡한 검증 로직으로 인해 발생하는 취약점이다. 공격자는 피해자의 ID 정보만 알고 있더라도, 미리 서명한 URL 을 통해 WebDAV API 의 인증을 우회하여 피해자 소유의 모든 파일에 대한 액세스 권한을 획득할 수 있다.

취약한 인증 로직은 SignedUrl 의 Verifier.php 에 존재하며, 해당 소스 코드는 서명된 URL 의 유효성을 검증하는데 사용한다.

```
public function signedRequestIsValid(): bool {
    $params = $this->getQueryParameters();
    if (!isset($params['OC-Signature'], $params['OC-Credential'], $params['OC-Date'], $params['OC-Expires'],
    $params['OC-Verb'])) {
        $q = \json_encode($params);
        \OC::$server->getLogger()->debug("Query parameters are missing: $q", ['app' => 'signed-url']);
        return false;
    }
    $urlSignature = $params['OC-Signature'];
    $urlCredential = $params['OC-Credential'];
    $urlDate = $params['OC-Date'];
    $urlExpires = $params['OC-Expires'];
    $urlVerb = \strtoupper($params['OC-Verb']);
    $algo = $params['OC-Algo'] ?? 'PBKDF2/10000-SHA512';

    unset($params['OC-Signature'], $params['OC-Algo']);
```

서명된 URL 검증 인자

그림 12. 서명된 URL 검증 인자

검증에 사용되는 인자들에 대한 설명은 다음과 같다. 이때, OC-Signature 값을 제외한 인자들은 임의의 값으로 설정 가능하며, OC-Signature 가 주요 검증 인자로 사용된다.

인자	설명	예시
OC-Signature	사용자의 서명 값	64 길이의 Hash 문자열
OC-Credential	사용자의 이름	admin, user 등등
OC-Date	서명 만료 날짜	2023-12-20
OC-expires	서명 유효기간	(기본 값) 1200
OC-Verb	HTTP Method 방식	GET, POST
OC-Algo	사용 알고리즘	PBKDF2 기반 sha512 반복 횟수 10000

OC-Signature 를 검증하는 verifySignature 로직을 살펴보면 computeHash 함수를 통해 검증을 수행하며, 사용자의 signingKey 를 기반으로 생성한 Hash 값과 OC-Signature 를 비교하여 사용자를 식별하는 것을 알 수 있다.

```php
private function verifySignature(array $params, $urlCredential, $algo, $urlSignature): bool {
    $trustedList = $this->config->getSystemValue('trusted_domains', []);
    $signingKey = $this->config->getUserValue($urlCredential, 'core', 'signing-key');
    $qp = \preg_replace('/%5B\d+%5D/', '%5B%5D', \http_build_query($params));

    foreach ($trustedList as $trustedDomain) {
        foreach (['https', 'http'] as $scheme) {
            $url = \Sabre\Uri\parse($this->getAbsoluteUrl());
            $url['scheme'] = $scheme;
            $url['host'] = $trustedDomain;
            $url['query'] = $qp;
            $url = \Sabre\Uri\build($url);

            $hash = $this->computeHash($algo, $url, $signingKey);
            if ($hash === $urlSignature) {
                return true;
            }
            \OC::$server->getLogger()->debug("Hashes do not match: $hash !== $urlSignature (used key:
            $signingKey url: $url", ['app' => 'signed-url']);
        }
    }

    return false;
}
```

그림 13. verysignature 함수

상세 분석을 위해 computeHash 함수를 살펴보면 사용자의 signingKey 를 조합하여, PBKDF2 알고리즘을 기반으로 SHA512 Hash 를 사용한 64 비트 길이의 서명 값을 생성하는 것을 알 수 있다.

```php
    protected function computeHash(string $algo, string $url, $signingKey) {
        if (\preg_match('/^(.*)\/(.*)-(.*)$/', $algo, $output)) {
            if ($output[1] !== 'PBKDF2') {
                return false;
            }
            if ($output[3] !== 'SHA512') {
                return false;
            }
            $iterations = (int)$output[2];
            if ($iterations <= 0) {
                return false;
            }
            return \hash_pbkdf2("sha512", $url, $signingKey, $iterations, 64, false);
        }
        return false;
    }
```

그림 14. computeHash 함수

취약한 버전의 ownCloud core는 사용자의 signingKey Default 값을 빈 문자열로 저장하고 있지만, 요청한 signingKey 값의 빈 문자열 여부를 확인하는 검증 로직이 누락되어 있다. 따라서, 공격자는 별도의 signingKey 를 입력할 필요 없이 PBKDF2-sha512 알고리즘 기반의 Hash 값을 임의로 생성해 서명된 URL 에 접근할 수 있으며, 인증 우회가 가능하다. 공격자는 이를 악용해 WebDAV 에 접근해 피해자 소유의 파일에 액세스 제어를 획득할 수 있다.

위의 정보를 기반으로 인증 우회 취약점을 통해 PoC 테스트에서 생성한 EQST_Lab.txt 에 접근하는 방법은 아래와 같다. 우선 임의로 서명된 URL 을 생성하기 위해 WebDAV URL 을 기반으로 한 OC-Signature 서명 Hash 값을 생성한다.

WebDAV 경로	**- WebDAV 경로** **[피해자 서버]**/remote.php/dav/files**/[사용자 ID]/[파일 경로]**?OC-Credential=**[사용자 ID]**&OC-Date=**[날짜]**&OC-Expires=**[만료 일자]**&OC-Verb=**[HTTP 메소드]** **- 실제 예시** 192.168.100.176:8080/remote.php/dav/files/eqst/Documents/EQST_Lab.txt?OC-Credential=eqst&OC-Date=2024-12-20&OC-Expires=1200&OC-Verb=GET

- Hash 생성 (참고 사이트: https://onlinephp.io/hash-pbkdf2)

그림 15. Hash 생성

공격자 서버에서 서명된 URL 의 나머지 값을 모두 추가하여 요청하면 파일에 접근할 수 있음을 확인할 수 있다.

명령어	**- 파일 접근 (GET 메소드)**
	$ curl 'http://192.168.100.176:8080/remote.php/dav/files/eqst/Documents/EQST_Lab.txt?OC-Credential=eqst&OC-Date=2024-12-20&OC-Expires=1200&OC-Verb=GET&OC-Signature=fed39dfd4203d17f220599b7f99fda4c7193c557ed257ec83d6ae009bed7594f'
	
	- 파일 탐색 (PROPFIND 메소드)
	$ curl -X PROPFIND "http://192.168.100.176:8080/remote.php/dav/files/eqst/Documents?OC-Credential=eqst&OC-Date=2024-12-20&OC-Expires=1200&OC-Verb=PROPFIND&OC-Signature=c566237b5b34e3490099a435c725f1c4a8f8f5c8e1cb7b3b9631fa06f36220ee"

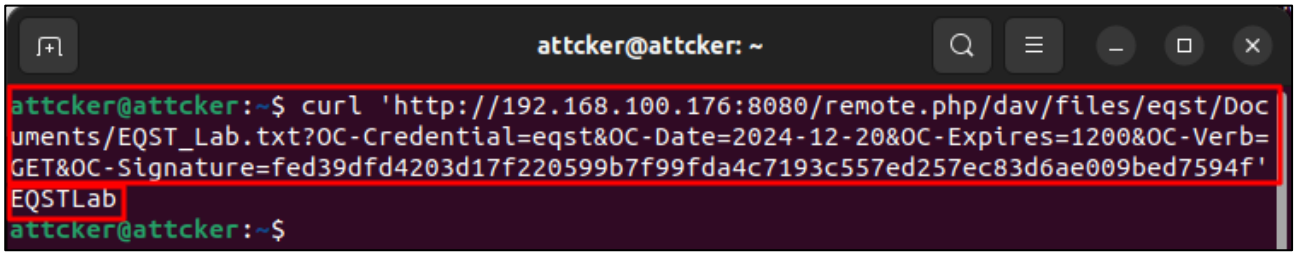
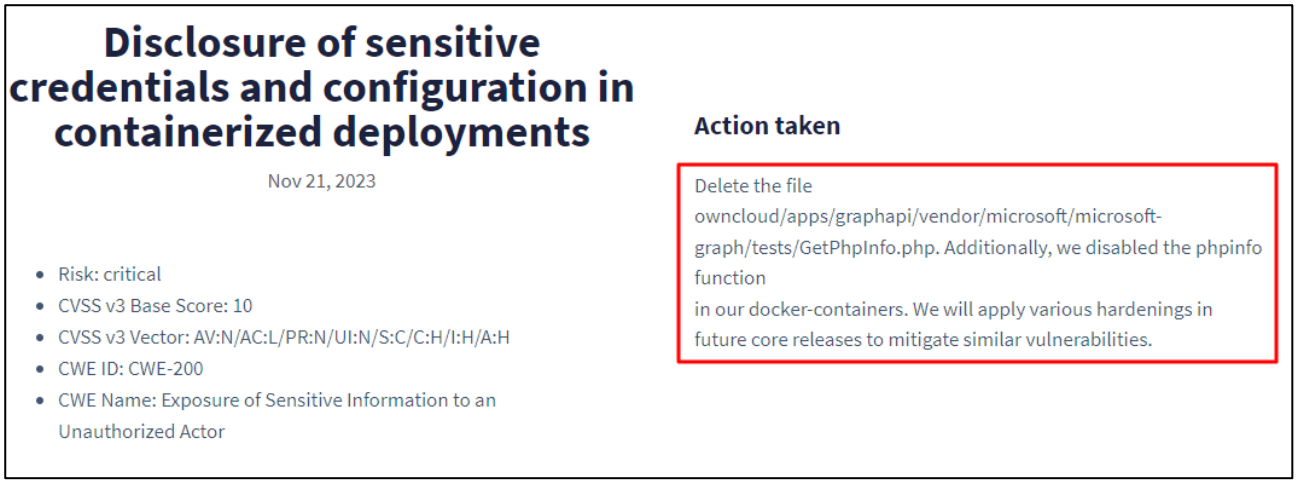


그림 16. 인증 우회를 통한 파일 접근

■ 대응 방안

1) 정보 노출 취약점(CVE-2023-49103)

취약한 버전의 ownCloud 이용 시, 계정 정보 탈취 및 민감 정보 유출뿐만 아니라 크리덴셜 스터핑, 클라우드 자격 증명 악용 등 잠재적인 시스템 손상도 발생할 수 있다. 따라서 이를 방지하기 위해 GetPhpInfo.php 파일 삭제 및 phpinfo 기능의 비활성화 패치가 진행된 graphapi 0.3.1 이상 버전으로 업데이트를 진행해야 한다.



출처: ownCloud 공식 홈페이지

그림 17. 정보 노출 취약점 패치 내역

불가피하게 버전 업데이트가 어려울 경우 패치내용과 동일하게 해당 GetPhpInfo.php 함수를 수동으로 비활성화 하거나 삭제해 예방할 수 있다.

2) 인증 우회 취약점(CVE-2023-49105)

취약한 버전의 ownCloud 를 사용하는 경우, 서명된 URL 을 통해 WebDAV API 를 우회하여 피해자가 소유한 파일에 액세스, 수정 및 삭제가 가능하다. 따라서, 파일 소유자가 서명 키를 구성하지 않은 경우, 미리 서명된 URL 을 통한 접근이 불가능하도록 패치한 ownCloud 10.13.1 이상 버전으로 업데이트를 진행해야 한다.

```
private function verifySignature(array $params, $urlCredential, $algo, $urlSignature): bool {
    $trustedList = $this->config->getSystemValue('trusted_domains', []);
    $signingKey = $this->config->getUserValue($urlCredential, 'core', 'signing-key');
    // in case the signing key is not initialized, no signature can ever be verified
    if ($signingKey === '') {
        \OC::$server->getLogger()->error("No signing key available for the user $urlCredential. Access via
        pre-signed URL denied.", ['app' => 'signed-url']);
        return false;
    }
    $qp = \preg_replace('/%5B\d+%5D/', '%5B%5D', \http_build_query($params));

    foreach ($trustedList as $trustedDomain) {
        foreach (['https', 'http'] as $scheme) {
            $url = \Sabre\Uri\parse($this->getAbsoluteUrl());
            $url['scheme'] = $scheme;
            $url['host'] = $trustedDomain;
            $url['query'] = $qp;
            $url = \Sabre\Uri\build($url);
```

빈 서명 값 검증 로직

그림 18. 인증 우회 취약점 패치 내역

불가피하게 버전 업데이트가 어려울 경우 사용자는 수동으로 서명 키를 생성하는 것으로 해당 취약점을 예방할 수 있다.

두 취약점 모두 공개된 ownCloud 서버를 대상으로 악의적인 사용자가 접근하여 악용이 가능한 취약점이다. 따라서, 두 취약점뿐만 아니라 앞으로 발생 가능한 취약점으로부터 선제적으로 대응할 수 있도록 OWNCLOUD_TRUSTED_DOMAINS 설정을 통해 접속 허용 IP 목록을 관리해 안전한 접근 제어 환경을 구축하여 사용하는 것을 권고한다. 이러한 조치를 적용한다면 안전성을 높이고 서버 보안을 강화할 수 있을 것이다.

■ 참고 사이트

• URL : https://www.labs.greynoise.io//grimoire/2023-12-05-owncloud-again-again/

• URL : https://www.ambionics.io/blog/owncloud-cve-2023-49103-cve-2023-49105

• URL : github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/gather/owncloud_phpinfo_reader.md

EQST INSIGHT

2024.01

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

발행인 : SK쉴더스 EQST사업그룹
제　작 : SK쉴더스 커뮤니케이션그룹