CVE-2022-39299 (Passport-SAML 취약점) (CWE-347)

- CVSS 점수 : 7.4-8.1 (버전 3.1)

- Passport-SAML은 Node.js 인증 라이브러리인 Passport를 위한 SAML 2.0 인증 공급자이다.
    - 원격 공격자는 passport-saml을 사용하여 웹 사이트에서 SAML 인증을 우회할 수 있다.
        - 공격이 성공하려면 공격자가 임의의 IDP 서명 XML 요소를 소유해야 한다.
            - 사용된 IDP에 따라 서명된 메시지 생성이 트리거 될 수 있는 경우 완전히 인증되지 않은 공격 (예 : 유효한 사용자에 대한 엑세스 없음)도 실행 가능할 수 있다.

- 즉, 이를 정리하여 설명하자면, CVE-2022-39299 취약점은 원격 공격자가 임의의 IDP 서명 XML 요소를 조작하여 Passport-saml을 사용하는 웹 사이트에서 SAML 인증을 우회할 수 있도록 하는 취약점이다.
    - 해당 취약점은 성공적인 공격으로 인하여 인증 메커니즘을 우회할 수 있고, 잠재적으로 무단 액세스 및 데이터 침해로 이어질 수 있다.
        - 또한, 이러한 취약점은 암호화 서명 검증의 결함으로 인하여 주로 발생하며, 공격자는 SAML 인증을 우회하기 위하여 악의적으로 서명된 XML 요소를 제작할 수 있다.

IDP란?

- Identify Provider의 약자로 ID 공급자를 의미한다.
    - 디지털 ID를 생성, 저장 및 관리하는 시슽템을 말한다. (사용자 인증 서비스의 줄임말로 사용되기도 한다.)

영향을 받는 패키지

- node/saml/node-saml (npm)
  - 영향을 받는 버전 : 4.0.0-beta.5 이하
  - 패치된 버전 : 4.0.0-beta.5 이상
- node-saml/passport-saml (npm)
  - 영향을 받는 버전 : 4.0.0-beta.3 이하
  - 패치된 버전 : 4.0.0-beta.3 이상
- node-saml (npm)
  - 영향을 받는 버전 : 4.0.0-beta.5 이하
  - 패치된 버전 : 4.0.0-beta.5 이상
- passport-saml (npm)
  - 영향을 받는 버전 : 3.2.2 이하
  - 패치된 버전 : 3.2.2 이상

- 성공적인 공격을 위해서는 공격자가 임의의 IDP 서명 XML 요소를 보유해야 하며, 이를 통하여 SAML 인증 메커니즘을 우회할 수 있다.
  - 사용된 IDP에 따라서, 서명된 메세지 생성이 트리거될 수 있는 경우, 완전히 인증되지 않은 공격 (즉, 유효한 사용자에 대한 엑세스 없음)도 실행 가능할 수 있다.

```
// Check if this document has a valid top-level signature
    let validSignature = false;
    if (this.options.cert && this.validateSignature(xml, doc.documentEleme
      validSignature = true;
    }
```

  - ValidatePostResponse 취약성 검사는 위의 함수 내에 있다. (passport-saml-2.0.0/src/passport-saml/saml.ts:775)
    - 특히 전체 XML 문서에 유효한 서명이 포함되어 있는지 validateSignature로 확인한다.

- 속성은 문서의 첫 번째 루트 노드를 반환한므로 첫 번째 루트 요소에서만 서명을 확인한다. (`doc.documentElement, documentElement`)

```
const assertions = xmlCrypto.xpath(doc, "/*[local-name()='Respor
const encryptedAssertions = xmlCrypto.xpath(doc,
                            "/*[local-name()='Response']/*[local-name()='I

if (assertions.length + encryptedAssertions.length > 1) {
  // There's no reason I know of that we want to handle multiple ass
  //   potential risk vector for signature scope issues, so treat this as
  throw new Error('Invalid signature: multiple assertions');
}
```

  - 해당 함수는 XML 내에 단 하나의 어설션만 있는지 확인하여 계속 진행한다.
    - 결과적으로 XML 파서는 여러 루트가 있는 XML 문서를 파싱하고, 서명은 하나의 루트 노드에만 적용될 수 있는 반면, XPath는 여러 루트 노드를 탐색하여 인증 및 권한 부여 요소를 찾을 수 있다.
      - 결론적으로, 하나의 루트 노드가 서명될 수 있다. (예 : 일반 SAML 오류 메세지) 그런 다음 서명되지 않은 다른 노드가 수정 가능한 인증 및 권한 부여 정보를 포함할 수 있다.
        - 이런 식으로 공격자는 인증 정보를 변조하고 tenent 내의 모든 계정에 엑세스 할 수 있다.
          - 참고로 익스플로잇 성공 여부는 passport 라이브러리 사용과 관련된 내부 인증 로직에 달려 있다.
            - 인증 로직에서 발생하는 authenticated-session 객체를 완전히 신뢰하는 경우 `passport.authenticate(...PASSPORT-SAML_OPTIONS...)` 취약할 가능성이 높다.

패치 및 해결 방법

- 사용자는 passport-saml 버전 3.2.2 이상으로 업그레이드 해야하며, 해당 문제는 4.0.0 beta.5 이전의 “node-saml” 베타 릴리스에서도 발생했다.
  - 업그레이드 할 수 없는 경우 SAML 인증을 비활성화하여 해결 방법을 찾을 수 있다.

Reference

- **https://github.com/node-saml/passport-saml/security/advisories/GHSA-m974-647v-whv7**
- **https://github.com/node-saml/passport-saml/commit/8b7e3f5a91c8e5ac7e890a0c90bc7491ce33155e**