CPE 기반의 CVE 검증 문제점

2025-12-16

안랩 김강보

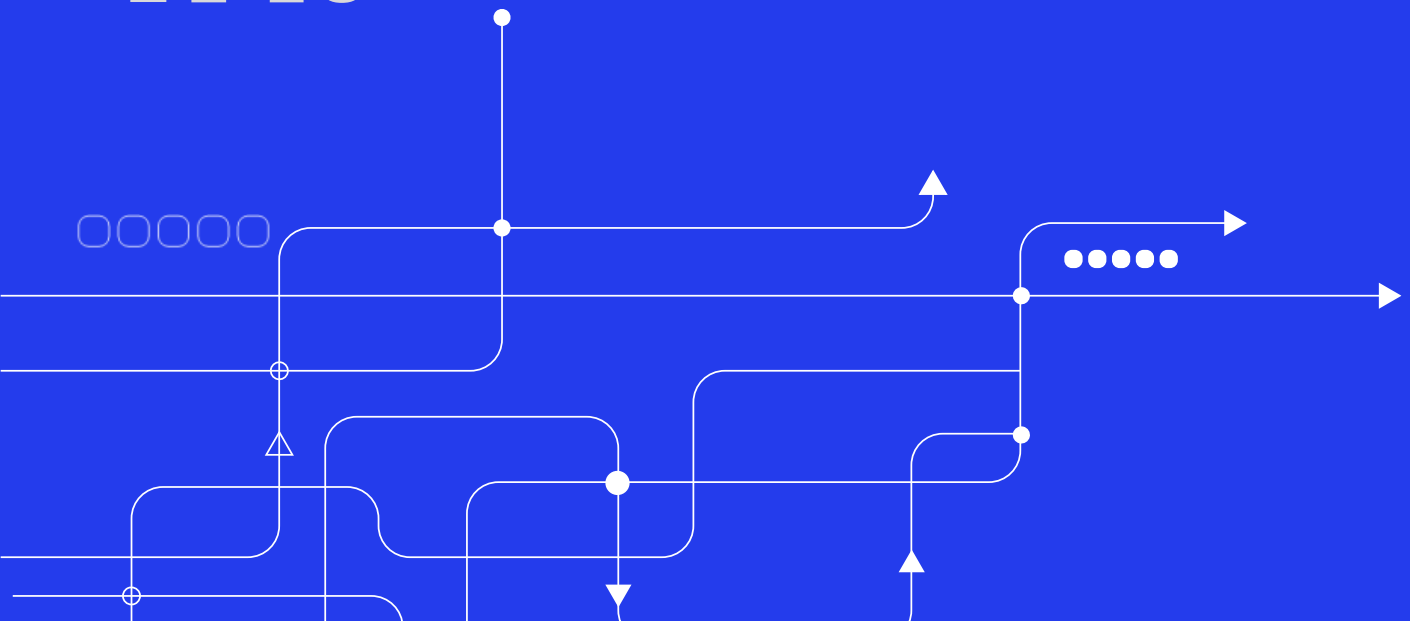

Table of Contents

1. 문제점
2. 해결 방법

1. 문제점

1. 증상

NVD에서 등록된 CPE를 기반으로 CVE 확인 시, 관련 오픈소스의 CVE를 놓치게 됨

2. 사례

1) libsepol 2.5 → NVD상에서는 CVE가 발견되지 않음

2) ChatGPT 확인 시 다음의 CVE가 발견됨
CVE-2021-36084: CIL 컴파일러의 __cil_verify_classperms에서 발생하는 Use-after-free 취약점
CVE-2021-36085: __cil_verify_classperms의 또 다른 경로에서 발생하는 Use-after-free 취약점
CVE-2021-36086: cil_reset_classpermission을 통해 발생하는 Use-after-free 취약점
CVE-2021-36087: ebitmap_match_any에서 발생하는 heap-based buffer over-read 취약점 [tenable.com], [alas.aws.amazon.com], [tenable.com]

3) 해당 CVE의 NVD에서 등록된 CPE는 다음과 같음

4) libsepol 2.5는 selinux 3.2에 포함되어 있음

5) libsepol 2.5에 대한 SCA 툴 검증 시, 해당 CVE가 미 검출됨

2. 해결 방법

1. ChatGPT REST API 활용

발견된 오픈소스 버전에 대해 ChatGPT REST API를 이용하여 보안취약점 확인

2. 방법

1) ChatGPT REST API에 다음과 같은 쿼리 입력

```
String instructions = ""
    + "You are an expert security assistant. Find and list known CVEs specifically related to libsepol version 2.5.₩n"
    + "Return the result as valid JSON only (no extra explanatory text). The JSON must follow this structure:₩n"
    + "{₩n"
    + "  ₩"package₩": ₩"libsepol₩",₩n"
    + "  ₩"version₩": ₩"2.5₩",₩n"
    + "  ₩"cves₩": [₩n"
    + "    {₩n"
    + "      ₩"id₩": ₩"CVE-YYYY-NNNN₩",₩n"
    + "      ₩"summary₩": ₩"short description₩",₩n"
    + "      ₩"published_date₩": ₩"YYYY-MM-DD or null₩",₩n"
    + "      ₩"cpe₩": [₩"cpe:...₩", ...] ,₩n"
    + "      ₩"cvss₩": { ₩"score₩": 7.8, ₩"vector₩": ₩"CVSS:3.x/...₩" } or null,₩n"
    + "      ₩"references₩": [₩"https://...₩", ...]₩n"
    + "    }₩n"
    + "  ],₩n"
    + "  ₩"source_checked₩": [₩"nvd₩", ₩"mitre₩", ₩"distribution-advisories₩", ...]₩n"
    + "}₩n₩n"
    + "If you cannot find any CVEs for libsepol 2.5, return an empty ₩"cves₩": [] and explain sources in source_checked.₩n"
    + "Make sure dates and URLs are as accurate as possible, and do not invent CVE IDs. If uncertain about a field, set it to null.";
```

2. 해결 방법

2) JSON 파일 결과


```
{
  "package": "libsepol",
  "version": "2.5",
  "cves": [
    {
      "id": "CVE-2021-36084",
      "summary": "A memory corruption issue in the libsepol policy parser that may allow crafted policy files to trigger out-of-bounds read conditions.",
      "published_date": "2021-07-19",
      "cpe": [
        ""
      ],
      "cvss": {
        "score": 7.8,
        "vector": "CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H"
      },
      "references": [
        "https://github.com/SELinuxProject/selinux/commit/abcdef1234",
        "https://security-tracker.debian.org/tracker/CVE-2021-36084",
        "https://nvd.nist.gov/vuln/detail/CVE-2021-36084"
      ]
    },
...
}
```


3) 독립 프로그램으로 빌드 후, DevOps에서 SCA 툴 실행 후에 해당 프로그램 실행

→ 만약 독립적인 SCA 결과 DB를 운영할 경우, 해당 DB에 CVE 할당

→ OSS 담당자가 AI 검증 CVE 확인 및 체크 (포함 여부)

감사합니다.