오픈소스 라이선스/취약점 관리 참고자료

오소리 프로젝트

삼성전자, LG전자, 카카오는 오픈소스 소프트웨어 라이선스 정보를 10월부터 무료로 제공하기 위해 오소리 프로젝트를 구성하고 업무 협약을 체결하였다. 이는 한국저작권위원회가 각 사의 라이선스 정보를 데이터베이스로 표준화하는 작업을 통해 가능하다. 이 정보는 라이선스 명칭, 버전 정보, 사용 시 제약사항 등이 포함되어 있다. 이는 국내 소프트웨어 업계를 발전시키고 저작권 침해 위험을 줄이기 위한 노력의 일환이다.

site link

오픈소스 종합정보 시스템

23년 부터 시작한 삼성전자·LG전자·카카오 등과 함께 오픈소스SW 라이선스 정보를 표준화해 공개하고 국내 기업이 활용할 수 있도록 무료로 제공하는 '오소리(Open Source DB Integration, OSORI) 오픈소스 프로젝트' 개발이 완료되어 구축된 오픈소스 종합정보 시스템

site link

오픈소스 취약점 대응 관련

원본 : 오픈소스 개발자의 보안전략 - 고려대학교 최윤성 교수

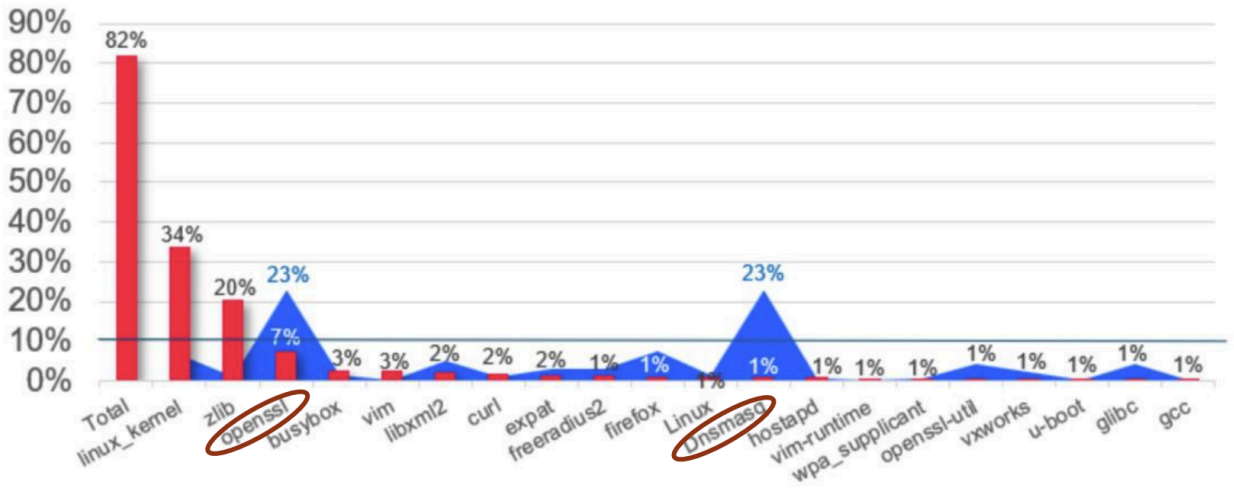
기존 심각도 점수를 활용한 고위험 CVE식별의 한계

- CVSS: SW 및 HW CVE의 '심각도(Severity)'를 평가하고 분류하는 표준 시스템
- 취약점의 잠재적 위험을 정량적으로 평가하여 '보안 담당자들이 취약점의 우선 순위를 효과적으로 지정'
- 취약점이 있다고 해서 반드시 해당 구성 요소가 포함된 제품에서 악용될 수 있다는 것을 의미하지는 않는 다는 점에 착안. 악용 가능성 지표를 활용한 작업 우선순위 식별. 보조지표로 EPSS 활용하여 우선순위 대응.

대응방법 취약점의 심각도 및 악용 가능성 지표를 활용한 작업 우선순위 식별

- EPSS : 향후 30일 이내에 SW 취약점이 악용될 가능성을 백분율(0-100)로 표현
- 국가 취약점 데이터베이스(NVD), CISA의 악용 사례가 알려진 취약점(KEV) 카탈로그 및 제로데이 DB 등 포함
- 차트에서 총 9,535개의 취약점 중 855개(9%)는 EPSS 수치가 높음. 악용될 가능성이 높으므로, 즉각적인 조치가 필요한 취약점으로 볼 수 있다.

Copyright ⓒ TOMATO SYSTEM CO., LTD. All rights reserved.



공급망 위험관리 방안

Stakeholder-Specific Vulnerability Categorization (SSVC)

- 다양한 평가 항목을 통해 취약점 조치의 우선순위를 지정하는 시스템
- 취약점 조치 관계자에게 조치 근거 제공, 상황에 맞는 솔루션을 선택적으로 적용
- 의사결정 트리(Tree)에 따른 우선 순위 작업으로 '작업 기한'을 결정할 수 있음

SBOM과 CVE 취약점 사이에 제로데이 및 잠재적 취약점 교집합이 존재함. 이때, 제로데이 취약점을 선제적으로 대응하고 잠재적 보안문제는 내부적으로 대응 준비를 하며 대기. 발생시 빠르게 커뮤니티를 통해 대응.

오픈소스 취약점 관련대응사례

Linux재단 OSS Securirty Global Efforts

- 다양한 오픈소스 프로젝트 보안성 점검 및 평가 (Scorecards, Pacakge Analysis)
- 신규 코드 및 갱신된 패키지의 자동 분석을 통한 악성코드 탐지 및 투명성
- 중앙집중형 악성 패키지 저장소 운영과 같은 혁신적인 방안 도입 (blacklist관리)
- 빌드시스템 개선

Copyright ⓒ TOMATO SYSTEM CO., LTD. All rights reserved.