소프트웨어 개발 기반 확보

국가 주도의 사이버 공격과 악의적인 온라인 이용자들이 급증하는 오늘날, Google 제품 및 서비스의 뛰어난 보안 수준은 이용자를 안전하게 보호하는 데 도움을 줍니다. Google은 이용자, 조직 및 정부를 보호하는 데 그 어느 때보다 주력하고 있습니다. 끊임없이 증가하는 사이버 범죄에 대처할 수 있도록 Google의 전문 지식을 공유하고 사회에 힘을 보태고 있으며, 모두에게 더 안전한 세상을 만들기 위해 지속해서 최첨단 사이버 보안을 발전시키고 있습니다.

누구나 자유롭게 사용, 수정 및 구축할 수 있는 코드인 오픈소스 소프트웨어는 현대 인터넷의 기반입니다. 오픈소스 소프트웨어 개발의 세계에서는 자유롭게 솔루션을 공유하여 협력하며 신속한 혁신을 이룩합니다. 그러나 누구든지 디지털 세계에 액세스할 수 있도록 하는 개방성은 특히 보안 위협에 취약합니다.

당면 과제

오픈소스 소프트웨어는 모두의 관심사입니다

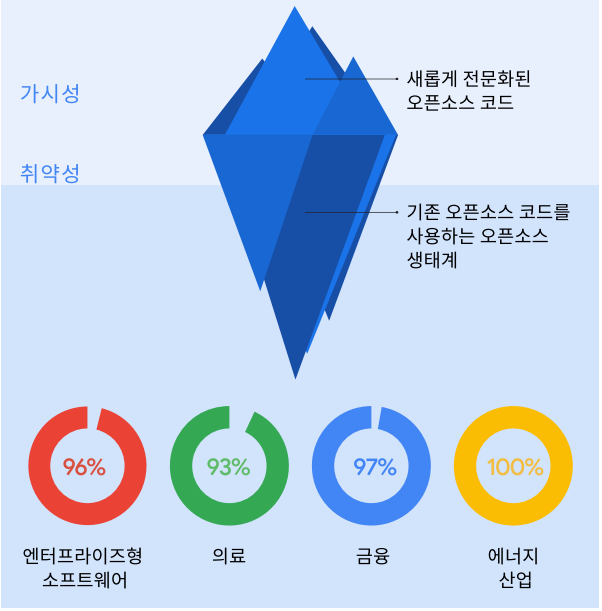
투명성과 공유를 기반으로 하는 오픈소스 개발 커뮤니티는 오늘날 사용하는 대다수의 애플리케이션에 방대한 양의 코드를 제공하고 있습니다. 사람들은 의료 장비부터 전력망까지 사이버 공격의 주요 타겟이 되는 오픈소스 프로젝트를 만드는 오픈소스 소프트웨어(OSS)에 사실상 매일 24시간 의존하고 있습니다. 소프트웨어 공급망 공격은 지난 3년간 매년 742% 증가[1] 했습니다.

오픈소스 생태계는 복잡하게 계층화되어 있으며 보이지 않는 간접 종속성 상의 보안 결함이 존재할 수 있습니다. 이러한 계층은 수동으로 취약점을 탐지하기 어렵게 만들기 때문에 소프트웨어 개발 시 이러한 부분을 보호하는 것이 세계적인 긴급 보안 문제로 부상했습니다.

모든 수준에서 추가적인 관심 필요

- 오픈소스 개발자에게는 프로젝트를 보호하는 지식과 리소스가 필요합니다
- 조직은 완화 방안을 세우기 위해 공급망 리스크 및 취약점을 이해해야 합니다
- 정부와 산업계는 강력하고 효과적인 보안 표준3을 보장하기 위해 협력해야 합니다[3]

오픈소스 코드를 보유한 업계 소프트웨어의 비율[2]



[2] 출처: 2022 Synopsys Open Source Security and Risk Analysis Report

Google의 해결 방법

모두를 위한 오픈소스 소프트웨어 보호

Google에서는 수년 동안 이 문제 해결에 몰두해 왔습니다. 실제로 매년 Google 직원(구글러)의 10% 이상이 오픈소스 소프트웨어 프로젝트에 참여합니다. Google의 경험에 따르면 현대의 디지털 보안은 실제로 개방성 수용을 통해 실현될 수 있다는 결론에 이르게 됩니다. 개방형 접근 방식으로 최신 혁신을 신속하게 도입할 수 있으며 더 많은 사람들이 보안 문제를 해결할 수 있기 때문입니다. 그러나 오픈소스의 가치를 충분히 높이려면 모두를 위한 보안을 강화하는 데 있어 더 강력한 공공 민간 파트너십 및 적극적인 정책 체계가 필요합니다. 이러한 이유로, Google은 2022년 상원에 제출된 오픈소스 소프트웨어 보호법 등 OSS 보안을 강화하고자 하는 미국 정부의 노력을 지지하고 있습니다.

- 또한 Google은 SLSA(소프트웨어 아티팩트용 공급망 레벨)[4,5] 등 차세대 보안 프레임워크를 통해 커뮤니티를 주도하며 고급 보안 도구를 개발하고 있습니다.
- 다른 소스의 소프트웨어 보안 정보를 쿼리 가능한 단일 데이터베이스로 통합하는 GUAC(아티팩트 구성 이해를 위한 그래프)를 개발하기도 했습니다. GUAC는 모든 조직에서 보안 정보에 자유롭게 액세스하고 유익하게 사용할 수 있도록 하여 그 가용성을 민주화합니다.

Google의 노력:

- 오픈소스 보안, Open Source Security Foundation의 임원직, 개발자와의 직접적인 협력에 미화 1억 달러 투자
- 내부에서 사용하는 실행 가능한 보안 표준, 지침, 무료 도구 및 모범 사례를 전체 오픈소스 커뮤니티를 통해 정의하고 공유
- 감지, 자동 선별 및 보안 구축 방법을 초기 개발 단계로 발전
- 자동화 툴링으로 모두가 엔터프라이즈급 보안에 무료로 액세스할 수 있도록 지원

애플리케이션

Google OSS Fuzz
하트블리드 버그에 대한 대응

하트블리드 버그는 거의 모든 인터넷 이용자에게 영향을 미치는 결함으로, 심각한 수준의 오픈소스 취약성을 나타냈습니다. 2014년, 이 버그를 사용한 해커가 미국 초대형 병원 중 하나의 데이터베이스에서 약 450만 명 분량의 환자 이름, 주소, 생년월일, 전화번호, 사회보장번호를 탈취했습니다

Google은 이에 대응하여 무료 커뮤니티 서비스로 OSS-Fuzz를 공개했습니다. 퍼즈 테스트는 몇 개월이 소요될 수 있는 수동 테스트와 다르게 알 수 없는 보안 약점을 정확히 찾아냅니다. Google은 수백 개의 오픈소스 프로젝트를 자동으로 테스트하는 인프라를 구축하는 데 투자했습니다. 현재 OSS-Fuzz는 주기적으로 코드 스캔을 실행하며 더 많은 버그를 찾기 위해 지속적으로 혁신하고 있습니다.

800개 이상의 중요한 오픈소스 프로젝트가 6개 국어로 된 퍼즈 테스트를 통해 스캔됩니다.

업계 투자 및 주요 성과

2020

8월
OpenSSF(오픈소스 보안 재단) 가입
오픈소스 소프트웨어 보안의 지도 및 개선을 목적으로 합니다.

2021

5월/6월
미국 행정 명령 14028호를 준수하는 **OSS 모범 사례를 확립**하고 소프트웨어 공급망 보안 표준에 기여했습니다.

6월
OpenSSF가 있는 SLSA 공개 Google의 내부 보안 프레임워크를 표면화하고 모두가 더 안전한 소프트웨어를 구축할 수 있도록 했습니다.

8월
OSS 향상 및 보호를 위해 미화 1억 달러 약속
개발자와의 협력을 통한 취약점 발견 및 수정을 포함합니다.

2022

5월
DC Summit 에서 **Google의 Open Source Maintenance Crew를 발표**했는데, 오픈소스 프로젝트를 통해 보안 개선에 직접적으로 협력하는 전임 개발자팀입니다.

5월
Assured Open Source Software 제품을 발표 Google이 사용하는 것과 동일한 신뢰도 높은 오픈소스 패키지를 개발자 워크플로에 통합하도록 지원합니다.

오늘날 공공 및 민간 조직의 보안을 유지하기 위한 Google의 권장 수칙:

- SLSA를 구현하여 소프트웨어 공급망 보안 강화
- Sigstore를 사용하여 암호화 서명 및소프트웨어의 정품 여부 확인
- OSS-Fuzz 및 OSV.dev를 통해 취약성 검색, 추적 및 심사 자동화
- 스코어카드 사용으로 종속성과 보안 위험을 자동으로 평가

Google의 접근 방식

소프트웨어의 보안 수준은 취약합니다. 전체 오픈소스 생태계의 보안을 강화하기 위해 전문 지식과 재원을 투자하고 있습니다. Google의 개발 및 보안 전문가팀은 다음과 같은 방법으로 더 많은 공공 및 민간 조직을 보호하고자 합니다.

Google은 제품 수명 주기의 전 단계를 심사하여 지속적으로 취약점을 스캔, 분석 및 퍼즈 테스트합니다

개방형 인터넷을 지원하여 개발자 커뮤니티에서 지식을 공유하고 이용자와 기업을 위해 보안을 유지합니다

교묘한 위협을 탐지하고 고급형 자동화 툴링을 제공하며 향후 발생할 보안 위협에 한발 앞서서 대비합니다.

오픈소스 소프트웨어 보호는 공동의 책임이며, Google은 이 긴급하고 중요한 문제에 지속적으로 협력할 것을 약속합니다. g.co/security/gosst

출처: 1. 2022 State of the Software Supply Chain. 2. 2022 Synopsys Open Source Security and Risk Analysis Report. 3. CISA Goes on Tour to Get Feedback on Cyber Incident Reporting Rules. 4. Google의 지식을 공유(즉, SLSA 공개, OpenSSF 안내)하면 Google뿐만 아니라 소프트웨어를 만드는 모두가 Google의 경험과 오래전부터 시행된 보안 수칙을 통해 이익을 얻을 수 있습니다. 5. SLSA는 조직이 소프트웨어 개발 프로세스의 보안을 개선하는 데 도움이 되는 일련의 관행입니다. 이는 사이버 보안에 관한 행정 명령에 대응하여 정부에서 제시한 요건인 미국 정부의 보안 소프트웨어 개발 프레임워크를 충족하는 데 도움이 됩니다. 즉, 조직에게는 연방 지침 준수 가이드가 생겨 이를 바탕으로 모두를 위해 더 안전한 소프트웨어를 만들 수 있습니다.