ソフトウェア開発の基盤を確保

国家が支援するサイバー攻撃や悪意のある攻撃者がオンラインで激増する中、Google の製品とサービスは安全性から切り離せないものだと考えています。Google では、専門知識を共有することにより、進化し続けるサイバーリスクに社会が対処できるようにしています。人々、組織、政府に対する保護をこれまで以上に重視しており、すべての人にとってより安全な世界を築くために、最先端のサイバーセキュリティを前進させる取り組みを継続的に行っています。

オープンソース ソフトウェアとは、誰もが自由に使用、変更、構築できるコードのことで、現代のインターネットの基盤となっています。オープンソース ソフトウェア開発の世界では、ソリューションを自由に共有することで、コラボレーションと急速なイノベーションが可能になります。しかし、オープンソースは誰もがアクセスできるデジタル世界を実現する一方で、セキュリティの脅威にさらされやすいという側面もあります。

課題

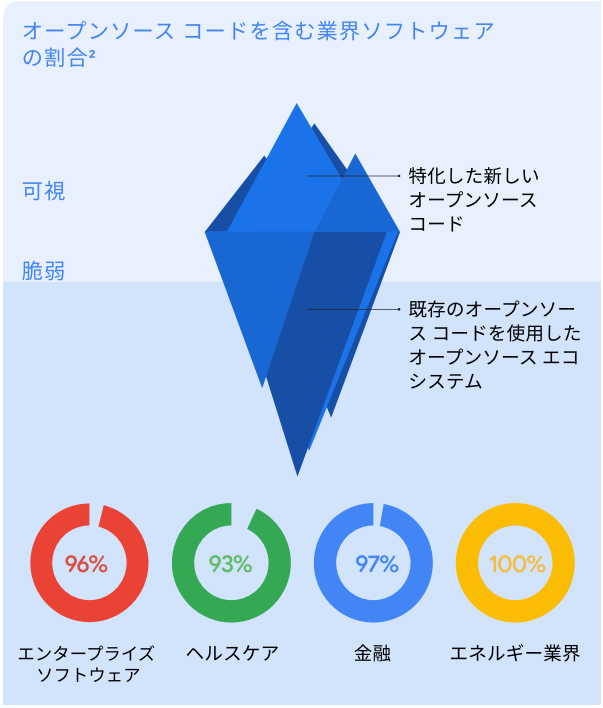
オープンソース ソフトウェアへの懸念は誰もが抱えるもの

透明性と共有を念頭に築かれたオープンソース開発コミュニティは、今日使用されているほとんどのアプリケーションに膨大な量のコードを提供しています。医療機器から送電網に至るまで、私たちは毎日毎時間オープンソース ソフトウェア（OSS）に依存しており、オープンソース プロジェクトはサイバー攻撃の主な標的となっています。過去 3 年間で、ソフトウェア サプライ チェーンへの攻撃は前年比で 742% 増加[1]しました。

オープンソース エコシステムは複雑に階層化されており、目には見えない間接的な依存関係にセキュリティ上の欠陥が含まれている可能性があります。このような階層のため、脆弱性を手動で検出するのは難しくなっており、この部分のソフトウェア開発を保護することは、世界的に緊急のセキュリティ問題になっています。

あらゆるレベルでより重視されるべきこと：

- オープンソース開発者は、プロジェクトを保護するための知識とリソースを必要としています。
- 組織は、サプライ チェーンのリスクと脆弱性を理解し、緩和策を策定する必要があります。
- 政府と業界は協力して、堅牢で効果的なセキュリティ基準を確保しなければなりません。[3]



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

Google のソリューション

すべての人のためにオープンソース ソフトウェアを保護する

Google では、この課題に何年も前から取り組んできました。実際に毎年 10% 以上の Google 社員がオープンソース ソフトウェア プロジェクトに貢献しています。その経験により、最新のデジタル セキュリティは、実際にはオープンにすることで実現できるとの結論が導かれました。オープンなアプローチにより、最新のイノベーションを迅速に採用し、より多くの人々がセキュリティの課題を解決できるようになります。しかし、オープンソースの価値を完全に解き放つには、より強力な官民パートナーシップと、すべての人のセキュリティを強化する動的なポリシー フレームワークが必要です。そのため Google は、2022 年に米国の上院で導入された Securing Open Source Software Act など、OSS セキュリティを推進する米国政府の取り組みを歓迎しています。

- Google は、Supply-chain Levels for Software Artifacts (SLSA),[4,5] や高度なセキュリティ ツールの開発など、次世代レベルのセキュリティ フレームワークでコミュニティを率いています。
- また Graph for Understanding Artifact Composition (GUAC) を開発しました。これにより、さまざまなソースからのソフトウェア セキュリティ情報がクエリ可能なひとつのデータベースにまとめられます。GUAC は、すべての組織が自由にアクセスできる有用なセキュリティ情報にすることで、その可用性を民主化するでしょう。

Google のコミットメント

- オープンソース セキュリティに 1 億ドルを投資、Open Source Security Foundation でのリーダーシップの役割、開発者との直接的なコラボレーション
- 社内で使用する実用的なセキュリティ基準、ガイダンス、無料ツールとベストプラクティス を定義し、共有する
- 高度な検出、自動トリアージ、セキュリティを開発の初期段階に組み込む方法
- ツールを自動化して、エンタープライズ レベルのセキュリティを無料で誰もが利用できるようにする

アプリケーション

Google OSS Fuzz
Google による Heartbleed バグへの対応

Heartbleed バグはオープンソースの重大な脆弱性であり、ほぼすべてのインターネット ユーザーに影響を与える可能性があるものでした。2014 年、ハッカーたちは米国最大の病院の 1 つのデータベースから約 450 万人の患者の名前、住所、生年月日、電話番号、社会保障番号を盗みました。

これに対して、Google は OSS-Fuzz を無料のコミュニティ サービスとして開始しました。ファズテストでは、数か月かかる手動テストとは異なり、未知のセキュリティの弱点が数分で特定されます。Google は、何百ものオープンソース プロジェクトを自動的にテストするためのインフラストラクチャの構築に投資しました。OSS-Fuzz は定期的なコードスキャンを実行するようになり、より多くの種類のバグの検出に向けて常に革新を続けています。

800 以上の重要なオープンソース プロジェクトをスキャンするファズテストは、6 つの言語で行われます。

業界への投資とマイルストーン

2020

8 月
Open Source Security Foundation (OpenSSF) に参加して、オープンソース ソフトウェアのセキュリティの指導と改善を行いました。

2021

5 月・6 月
米国大統領令 14028 に準拠した OSS のベストプラクティスを確立し、ソフトウェア サプライ チェーンのセキュリティ基準に関するガイダンスに貢献しました。

6 月
OpenSSF を使用した SLSA をリリースし、Google の内部セキュリティ フレームワークを外部化して、誰もがより安全なソフトウェアを構築できるようにしました。

8 月
OSS の向上と保護に 1 億ドルの投資を約束。これには、脆弱性の発見と修正に向けた開発者との提携が含まれます。

2022

5 月
DC Summit で Google の Open Source Maintenance Crew を発表し、専任の開発者チームがオープンソース プロジェクトのチームと直接連携してセキュリティを向上させました。

5 月
Assured Open Source Software 製品を発表しました。これは、Google も使用している信頼性の高いオープンソース パッケージを開発者のワークフローに組み込むためのものです。

Google が推奨する、公共と民間組織の安全を守るための現代的なプラクティス：

- SLSA を実装して、ソフトウェア サプライ チェーンのセキュリティを強化する
- Sigstore を使用して、ソフトウェアの信頼性を暗号化して検証する
- OSS-Fuzz と OSV.dev を使用して、脆弱性の検出、追跡、トリアージを自動化する
- スコアカードを使用して、依存関係のセキュリティ リスクを自動的に評価する

Google のアプローチ

ソフトウェアの安全性は、最も弱いリンクの安全性と同じです。Google は、オープンソース エコシステム全体のセキュリティを高めるために専門知識と財源を投資しています。開発とセキュリティの専門家からなる Google のチームは、次の方法でさらに多くの公的・私的な組織を保護できると考えています。

Google のチームは、製品ライフサイクルのすべての段階を監査し、脆弱性に対するスキャン、分析、ファズテストを継続的に行っています。

Google はオープンなインターネットをサポートし、社内の知識を開発者コミュニティとも共有することで公共と企業の安全性を確保しています。

Google は、巧妙な脅威を検出し、高度な自動化ツールを提供し、あらゆる可能性に事前に備えることで、未来のセキュリティを確実なものにしています。

オープンソース ソフトウェアの保護は共同責任です。Google は、この緊急かつ重大な問題について引き続き協力していくことをお約束します。g.co/security/gosst

ソース: 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.知識の共有（SLSA のリリース、OpenSSF を導くなど）により、Google だけでなく、ソフトウェアを作成するすべての人が、Google の経験と定評のあるセキュリティ プラクティスの恩恵を受けることができるようになります。5.SLSA は、組織がソフトウェア開発プロセスのセキュリティ向上に利用する一連のプラクティスです。これは、サイバーセキュリティに関する大統領令に応じて政府が定めた要件である、米国政府のセキュア ソフトウェア開発フレームワークを満たすことを目的に使用されます。SLSA により、組織は連邦政府のガイドラインに準拠して、ソフトウェアをすべての人にとってより安全にする方法に関するガイダンスを得ることができます。