GitHub

NEWS RELEASE

2021年1月5日
ギットハブ・ジャパン合同会社

1周年を迎えたGitHub Security Lab、新たな活動方針を発表

ソフトウェア開発者とセキュリティ研究者の相互関与強化を推進

オープンソースプロジェクトおよびビジネスユースを含む、ソフトウェアの開発プラットフォームを提供するGitHub, Inc.（本社：米国サンフランシスコ）は、12月18日（米国時間）に1周年を迎えたGitHub Security Labの新たな活動方針を発表しました。

GitHub Security Labは、昨年のGitHub Universeで発表され、1周年を迎えました。GitHub Security Labでは、オープンソースエコシステムを保護するために、リソース、ツール、報奨金を提供するとともに、セキュリティ研究に取り組んでいます。エコシステムの保護は、GitHubだけで解決できる課題ではありません。そのため、「オープンソースのセキュリティはすべての人にとって重要である」という私たちと同じ信念をもつ研究者、メンテナー、企業とともに、業界全体で連携すべきだと考えています。GitHub Security Labのミッションは、セキュリティ研究、コミュニティの構築、業界の積

極的な関与という、オープンソースソフトウェア(OSS)における3つの主軸に重点的に取り組むことです。

2020年は、Security Labにとっても、新しい課題とチャンスに満ちた激動の1年でした。その1年目のSecurity Labのハイライトをいくつかご紹介します。

セキュリティ研究

Security Labの主な取り組みは、OSSに潜む脆弱性が攻撃される前に検出するための研究です。CodeQLによるバリアント解析、ターゲットを絞ったファジング、手動でのコードレビューを通じて、GitHub Security Labはオープンソースコミュニティ全体で400件を超える問題を(組織的な開示を通じて)報告し、これまでに共通脆弱性識別子(CVE)が割り当てられたのは194件にのぼります。

GitHubは、下記のようなプロジェクトの脆弱性を報告しました。

- Google Chrome
- Android
- Linuxカーネル
- Ubuntu
- 多くのJavaエンタープライズアプリケーション

また、アクティブなサプライチェーン攻撃の阻止も支援し、最近では、ドイツの新型コロナウイルス感染症対応用インフラストラクチャにおける重大なリモート脆弱性の特定と修正にも貢献しました。
当社は、その取り組みが他の方々にインスピレーションを与えるだけでなく、セキュリティコミュニティの取り組みを開発コミュニティに返すことができる道筋を提供したいと考えています。だからこそGitHubでは、脆弱性を見つけたときに単にそれを報告するだけでなく、可能な限りCodeQLにクエリを投稿しています。これにより、開発者が今後同じ間違いをすることを防ぎます。

コミュニティの構築

コーディングはソーシャルなものであり、セキュリティも同様です。当社がコミュニティを構築しているのはそのためです。コミュニティでは、セキュリティ研究者が知識を共有したり、開発プラットフォームであるGitHubを使用して取り組みを拡大したり、従来のセキュリティ研究のルートを越えて開発者をサポートすることができます。

Security Labのバグ報奨金プログラムでは、研究者にバグの報告を依頼するだけでなく、これらのバグを大規模に自動検出するCodeQLクエリの作成も依頼しています。今年、GitHubは20名を超えるコントリビューターに対して報奨金として10万ドル以上を提供しました。こうした報酬の結果として作成されたクエリは現在、Code Scanningを使用して何十万ものオープンソースプログラムで継続的に実行され、脆弱性の再発を阻止しています。

コミュニティへの貢献をさらに促すために、GitHubは最近、影響の大きい報告に対する報奨金の額を倍増させました。OSSの長期的なセキュリティに貢献している研究者に対して、より大きな報奨

を提供したいと考えており、現在は重要な報告1件につき最大6,000ドルの報奨金を提供しています。

業界の積極的な関与

当社は、昨年のGitHub Security Labの発表と同時に、OSSの保護に尽力している世界中の企業と組織を1つにまとめるOpen Source Security Coalition(OSSC)も立ち上げました。その創設メンバーとして、Google、HackerOne、IOActive、Mozilla、Microsoft、NCC Group、Trail of Bitsなど、21社を迎え入れました。

OSSCには4つのアクティブなワーキンググループがあり、脆弱性の開示、オープンソースプロジェクトへの脅威の特定、オープンソース開発者向けのベストプラクティス、およびセキュリティツールに重点的に取り組んでいます。この取り組みはすぐに、OSSCとして初のレポート『*The Threats, Risks, and Mitigations in the Open Source Ecosystem*』へとつながりました。また、OSSCを推進する中で学んだ主要な教訓を共有しました。

また、数か月前には、こうした取り組みを足掛かりにして、OSSCは他のオープンソースセキュリティイニシアチブと提携し、Open Source Security Foundationを結成しました。GitHubはその創設メンバーとなっています。OpenSSFを通じて、GitHubは既にOpenSSF CVEベンチマークに貢献しています。これは、実世界のコードベースに基づいて静的アプリケーションセキュリティテスト(SAST)ツールを評価する新しいツールとデータのセットです。

Security Labは、業界の取り組みに継続的に関与していく中で、セキュリティ研究の社会技術面にも重点を置くようにその焦点を拡大しています。具体的には、脆弱性開示プロセスにおいてオープンソースのメンテナーとセキュリティ研究者がより適切にコミュニケーションを行うための方法を模索しています。

今後のGitHub Security Labについて

これまで194件のCVEを検出してきましたが、2021年のバグハントシーズンに新しいCVEをどれだけ検出できるかという競争がすでに始まっています。当社は、初年度に学んだ教訓を振り返りながら、当社の研究が開発者とセキュリティ研究者の両方のコミュニティにとって実用的な内容となることを目指し、新たに取り組んでいこうと考えています。

脆弱性を検出するのがGitHub Security Labあるいは他の誰であっても、当社はOSSの脆弱性を通知、修正、公表するワークフローを、セキュリティ研究者およびメンテナーがお互いにより協力し合える豊かなプロセスにしていくことができると確信しています。GitHubはセキュリティアドバイザリとアドバイザリデータベースを導入することで、プロセスをより良いものにすべく取り組んできました。Security Labにおいて当社が高く評価しているのは、セキュリティ研究者が脆弱性の検出に対してクレジット(称賛)を得られるようになったことです。2021年には、このOSS脆弱性ワークフローをコミュニティ全体が参加でき、信頼できるワークフローにできるよう、Security Labがより直接的に関与していきます。

GitHubではこの1年間、開発者が無意識に取り込んでしまった悪用可能なOSSの脆弱性の検出に重点的に取り組んできました。しかしながら、ネームハイジャックやマルウェアを介したOSSサプラ

イチェーン自体に対する攻撃の量はますます増加しています。こうした問題についても、当社がサポートできると考えています。

最後になりましたが、当社はこれからもセキュリティコミュニティと開発コミュニティの間の隔たりをなくすサポートをしていきたいと考えています。現在、CodeQLクエリはそれを実現するための1つのメカニズムであり、当社はこれからも尽力していきます。また、教育コンテンツの作成やコミュニティの取り組みへの参加という形でも、隔たりをなくしていくことができます(最も注目すべきはOpenSSFです)。GitHub Security Labへの参加については、こちらをご覧ください。

GitHub Blog
英語
https://github.blog/2020-12-18-happy-anniversary-github-security-lab/
日本語
https://github.blog/jp/2021-01-04-happy-anniversar%E2%80%A6hub-security-lab/

GitHubに関する情報は、こちらからもご覧いただけます。
Blog： (英語) https://github.blog (日本語) https://github.blog/jp
Twitter： (英語) @github(https://twitter.com/github)
(日本語) @GitHubJapan(https://twitter.com/githubjapan)

【GitHub について】https://github.co.jp
GitHub（ギットハブ）は世界で5,600万人にのぼる開発者および300万の組織に利用される開発プラットフォームです。プログラミング環境にオープンな会話と協調を重んじるコミュニケーションによって、コラボレーションを促進する開発環境を提供しています。これらの開発を実現するワークフローで必要となるコードレビュー、プロジェクトおよびチームマネージメント、ソーシャルコーディング、ドキュメント管理などに、これまで以上の効率性と透明性をもたらし、より高速かつ品質の高いソフトウェア開発を支援しています。
GitHubは多様なユースケースに適した開発プラットフォームを用意しており、オープンソースジェクトから企業における機密性の高いソフトウェア開発までに対応できます。無料で利用できるパブリックリポジトリは、オープンソースプロジェクトにて多く利用されています。プライベートリポジトリが利用できる有償サービスとして GitHub Enterprise や GitHub One などのプランも提供しています。
2008年に米国サンフランシスコで創業したGitHub, Inc.は、初の海外支社として、2015年に日本支社を開設しました。

【製品／サービスに関するお問い合わせ先】
ギットハブ・ジャパン営業およびサポート窓口
Email: jp-sales@github.com

【報道関係者からのお問い合わせ先】
ギットハブ・ジャパンPR事務局（プラップジャパン内）
担当：住川 / 西田
Email: GitHub@prap.co.jp