GitHub

NEWS RELEASE

2019年5月24日
ギットハブ・ジャパン合同会社

GitHub、ソースコードの安全性を維持する セキュリティ機能をリリース

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、ソフトウェア開発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、以下ギットハブ）は、5月23日に独ベルリンで開催した開発者向けのカンファレンスGitHub Satelliteにおいて、開発者が容易にソースコードの安全性を向上できる新たなセキュリティ機能を発表しました。

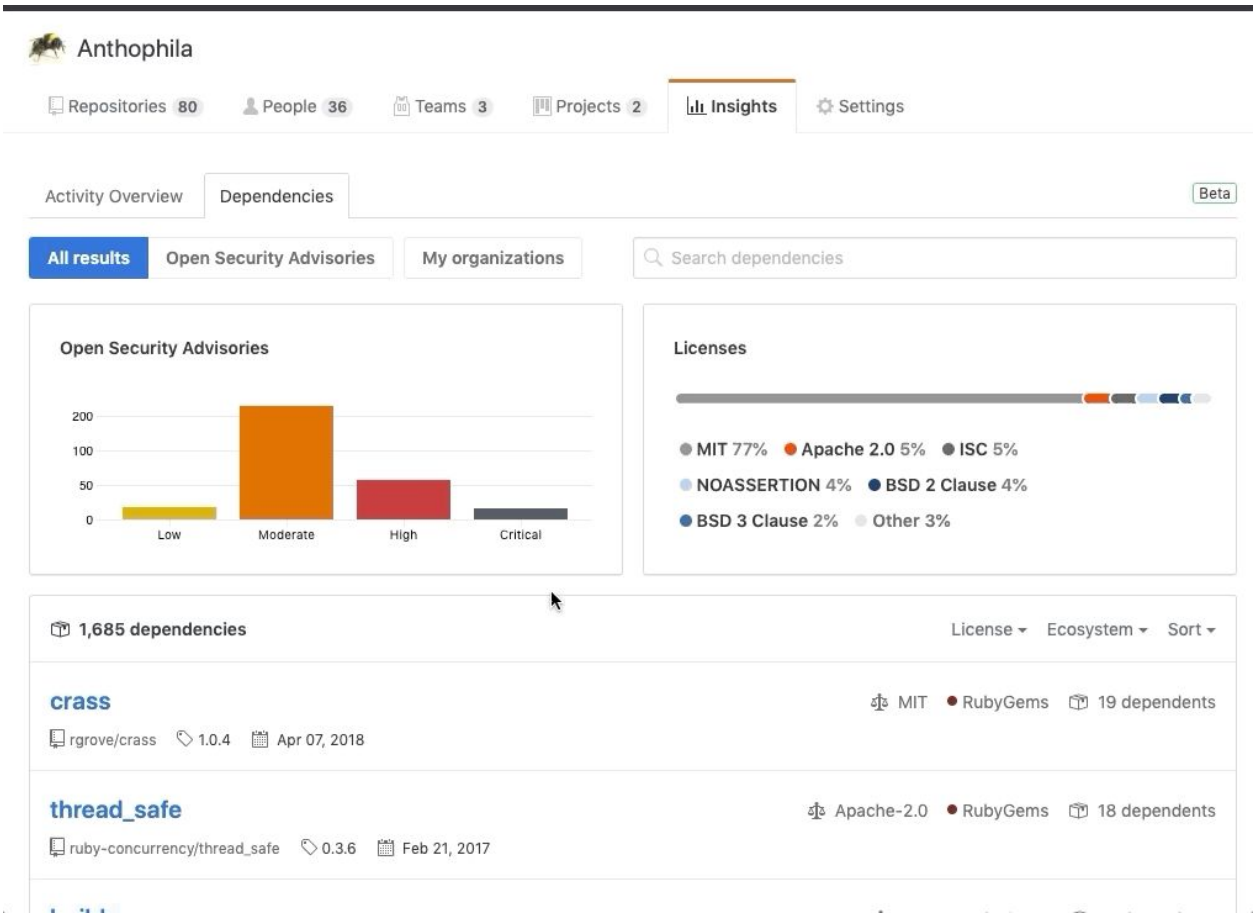
ソフトウェアの開発は、他のメンバーの作業に基づいて開発されています。新規のソフトウェアプロジェクトの99%にオープンソースコードが使用され、膨大な量のコードの再利用によって、かつて無いほどスピーディーにソフトウェアを開発できるようになっています。一方で、このような依存関係があるため、脆弱なソフトウェアが配布されてしまうと、ユーザ全員がリスクにさらされます。すべての開発者が、セキュリティに配慮する開発者になるという重要性が、これまで以上に高まっています。すなわち、誰もが脆弱性情報を開示し、パッチ処理を迅速に行う責任を負っています。

GitHubは、開発者が容易にソースコードの安全性を向上できる新たなセキュリティ機能を発表しました。

- WhiteSource社のデータによるセキュリティ脆弱性アラート：GitHubは、2017年にベータ版としてセキュリティアラート機能をローンチしました。ベータ版のリリース以来、.NET、Java、JavaScript、Python、およびRubyに関わる脆弱性が発見された依存関係に対して、約2,700万のセキュリティアラートを送信しています。WhiteSource社との新たなパートナーシップによってそのデータを活用し、オープンソースプロジェクトにおける潜在的な脆弱性

を発見する対象範囲が広がり、脆弱性修復のためのより詳しい情報提供が可能になりました。

- ディペンデンシー・インサイト：セキュリティの脆弱性が一般公開されると、企業はその依存関係を速やかに監査し、脆弱性の影響範囲を適切に把握するためのツールが必要となります。ディペンデンシー・インサイトを使うことで企業は脆弱性やオープンソースライセンスの詳細などの依存関係を完全に可視化できるようになります。



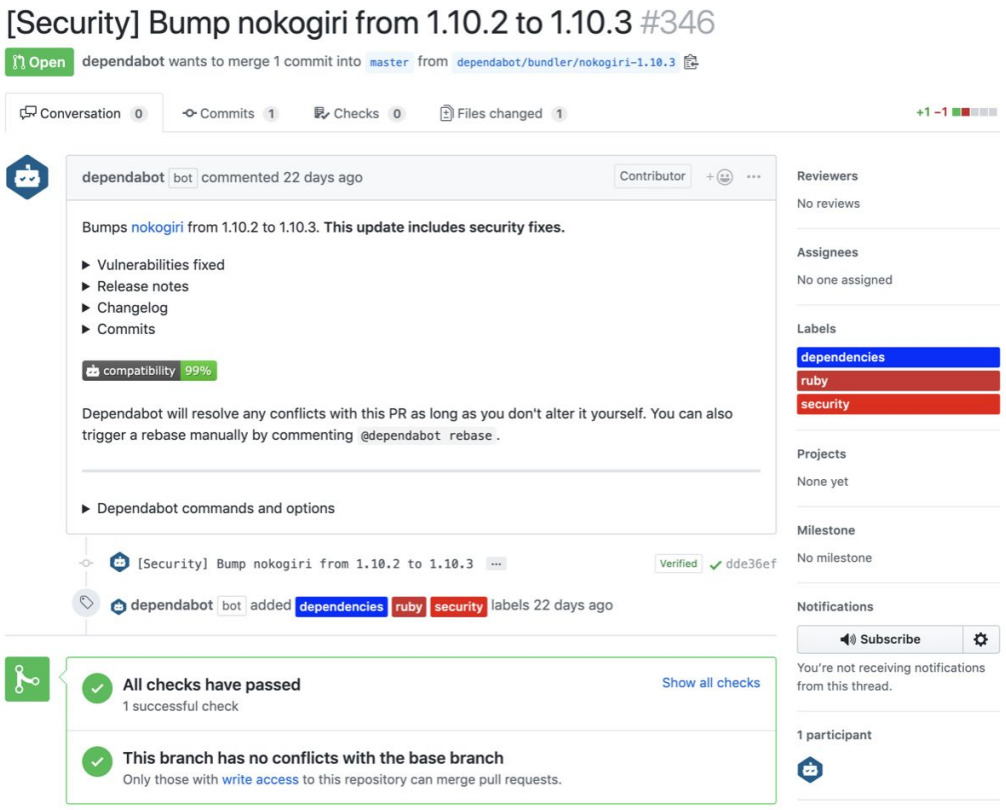
- トークン・スキャンニング：ベータ版としてリリースしていたトークン・スキャニングが正式版としてリリースされました。正式版では、誤ってチェックインしたことでデータ漏洩が生じないよう、Alibaba Cloud、Mailgun、Twilioを含む、より多くのトークンフォーマットをサポートしています。

Dependabotによるセキュリティパッチの自動化

業界データによると、脆弱性に関するアラートを通して、セキュリティ保護に関する情報が提供されていても、70%の脆弱性は30日後になってもパッチ対応が行われず、その多くは1年以上経過してから対応されていると報告されています。こうした中で、GitHubは依存関係の脆弱性対応を容易にするために、**Dependabotを買収**しGitHubに統合しました。Dependabotの統合により、既知の脆弱性に関わる依存関係を監視し、脆弱性が発見された場合はPull Requestを自動的に作成して最低限必要なバージョンに更新できるようになります。GitHubは、今後数ヶ月で、セキュリティアラー

トを有効にしているすべてのアカウントがこのような自動化されたPull Request機能を使えるように開発を進めます。

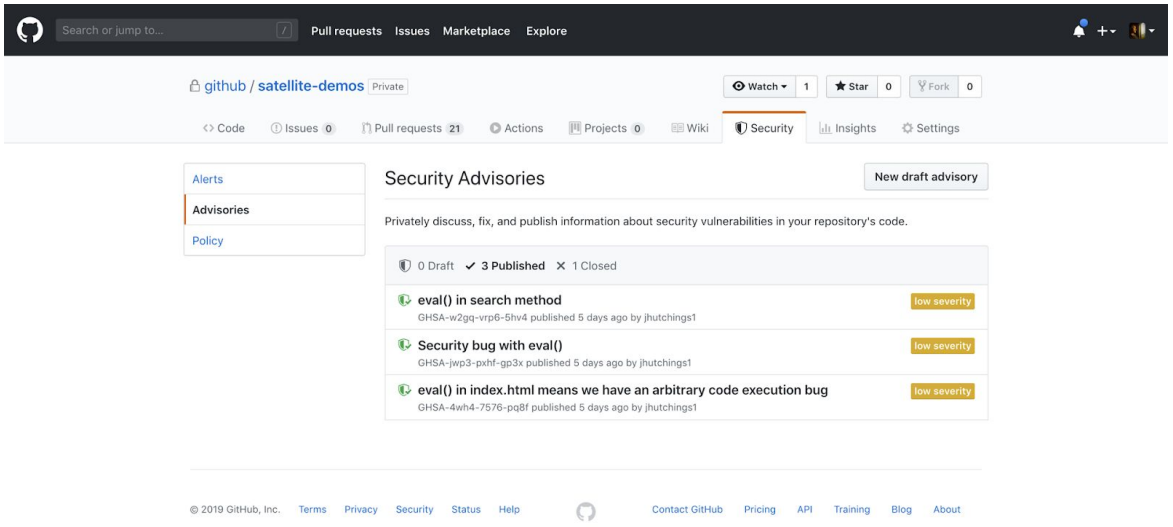
詳細はこちら



オープンソースのセキュリティ

バグが発生しないソフトウェアは存在しないと言えます。特に、オープンソースソフトウェアの世界では何千ものプロジェクトが依存関係にあるため、脆弱性が重大な影響を及ぼす可能性があります。大手ベンダーには、セキュリティ問題への対処に詳しい専任のセキュリティチームがいることもありますが、ほとんどのオープンソースのプロジェクトでは、そのようなチームはいません。こうした中で、メンテナがセキュリティの問題に非公開で対処し、責任を持って情報を開示できる新機能を発表します。

- メンテナ・セキュリティ・アドバイザリ(ベータ版)：オープンソースのメンテナがセキュリティの脆弱性に遭遇した場合、ユーザを保護するためにその問題に対処し、開示できる場が必要になります。GitHubは、メンテナが話し合い、問題を修正し、セキュリティアドバイザリを発表できる非公開のワークスペースを用意しました。このスペースを活用すればハッカーに情報が漏れることはありません。



- セキュリティ・ポリシー：セキュリティは私たち全員の責務です。現在は、善意のユーザがパブリックスペースにissueを作成し、メンテナにセキュリティのバグの疑いを知らせることがよくあります。セキュリティ・ポリシーでは、セキュリティに関するissueが作成された場合、issueを作成したユーザにコンタクトし、設定されたセキュリティポリシーに従うよう促すことができます。オーガナイゼーションでは、そのオーガナイゼーション配下のすべてのリポジトリに自動適用されるセキュリティポリシーを作成することもできます。

現在のソフトウェアが直面しているセキュリティの課題は、コミュニティの問題です。業界を牽引している開発者プラットフォームであるGitHubが保有するデータ量とユーザー数を考えると、GitHubはコミュニティを脅威から保護し、全員のセキュリティを強化する責任があります。今後も新機能への投資を継続し、様々なパートナーと協力して、GitHubのプラットフォームに業界のベストプラクティスをもたらします。

GitHub Blog
英語 https://github.blog/2019-05-23-introducing-new-ways-to-keep-your-code-secure/
日本語 https://github.blog/jp/2019-05-24-introducing-new-ways-to-keep-your-code-secure/

こちらからもGitHubに関する情報をご覧いただけます。
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)

【ギットハブについて】https://github.co.jp
GitHubは世界で3,600万人にのぼる開発者および210万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が、プライベートリポジトリが利用できる有償サービス、GitHub EnterpriseやBusiness on GitHub.comなども提供しています。
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／サービスに関してお問い合わせ先】
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

【報道関係者様からの連絡先】
ギットハブ・ジャパンPR事務局（旭エージェンシー内）
担当：牟田 / 西田
Email：GitHubJapan_pr@asahi-ag.co.jp Tel: 03-5574-7890