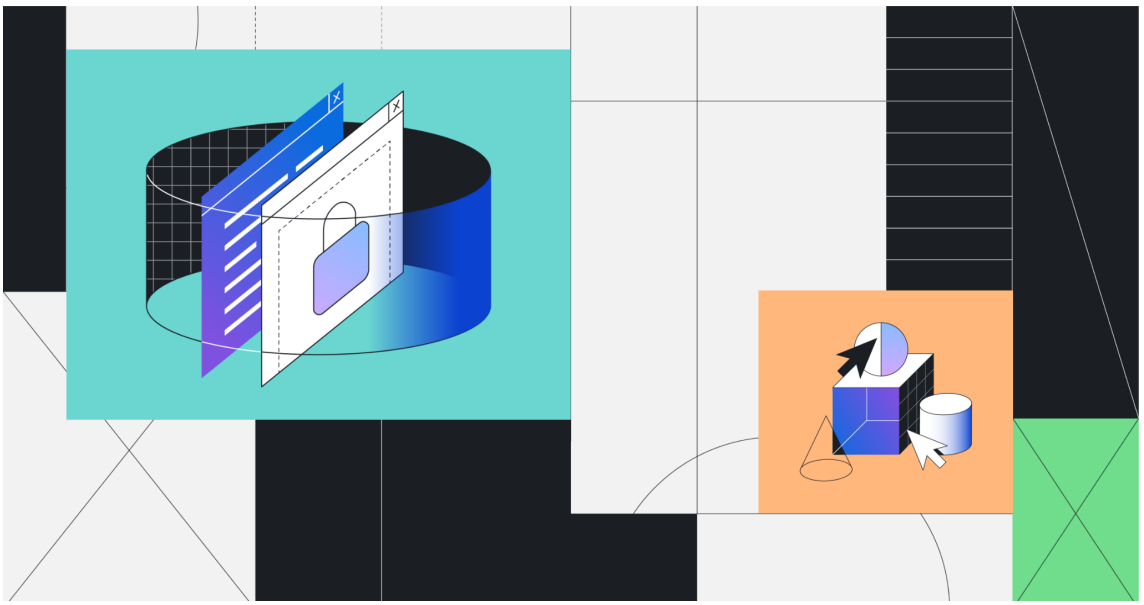
GitHub

NEWS RELEASE

2022年8月29日
ギットハブ・ジャパン合同会社

GitHub Actionsのワークフローに存在する脆弱性をDependabotで告知

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、8月9日（米国時間）に、GitHub Actionsのワークフローに存在する脆弱性をDependabotで告知すると発表しました。



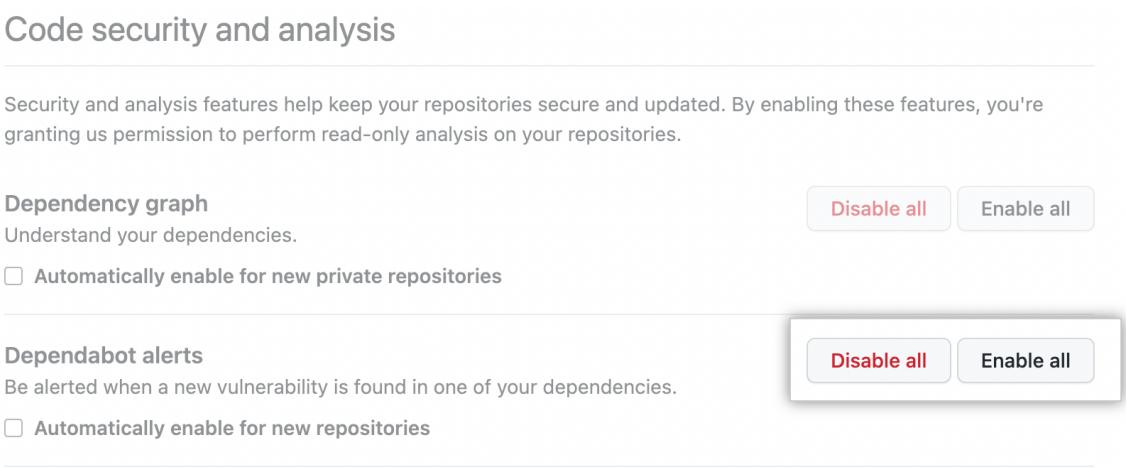
ソフトウェア開発チームが、さらに多くのソースコードを開発し、迅速にリリースするためには、開発環境上に構築された安全なCI/CDワークフローは非常に重要な要素です。

このたび、GitHubに実装されているCI/CDツール、GitHub Actionsのワークフローに存在する脆弱性に対して、Dependabotアラートを送信できるようになりました。これにより、今までよりも簡単に、GitHub Actionsワークフローで最新の状態を維持し、セキュリティの脆弱性を修正できるようになります。このアラートには、GitHub Advisory Databaseが利用されています。GitHub Actionsのワークフローに含まれるセキュリティの脆弱性が報告されると、セキュリティ研究者のチームが脆弱性を文書化し、アドバイザリを作成します。これにより、影響を受けるリポジトリに対して、アラートが通知されます。GitHub Advisory Databaseのすべてのデータと同様に、これらのアドバイザリも検索可能で、永久に無料で利用可能です。

GitHub NEWS RELEASE

GitHub Actionsに対するDependabotアラート

影響を受けるGitHubリポジトリへのDependabotアラートは、GitHub Advisory Databaseを利用して実施されます。Dependabotを既にお使いの場合は、設定変更などは不要で利用できます。ソースコードに影響を及ぼすGitHub Actionsと脆弱性に対するアラートを受け取るには、[Code security and analysis (コードのセキュリティと分析)]タブで、[Enable all (すべて有効化)]を選択し、Dependabotを有効に設定してください。



GitHub Actionに対するアドバイザリの報告

GitHub Actionのオーナーとして脆弱性を発見した際は、リポジトリの[Security (セキュリティ)]タブからアドバイザリの作成プロセスを開始できます。GitHub Actionエコシステム内でリポジトリアドバイザリが作成され、タグ付けされると、GitHubのキュレーションチームがリポジトリアドバイザリを確認し、誤りが無ければグローバルアドバイザリを作成します。

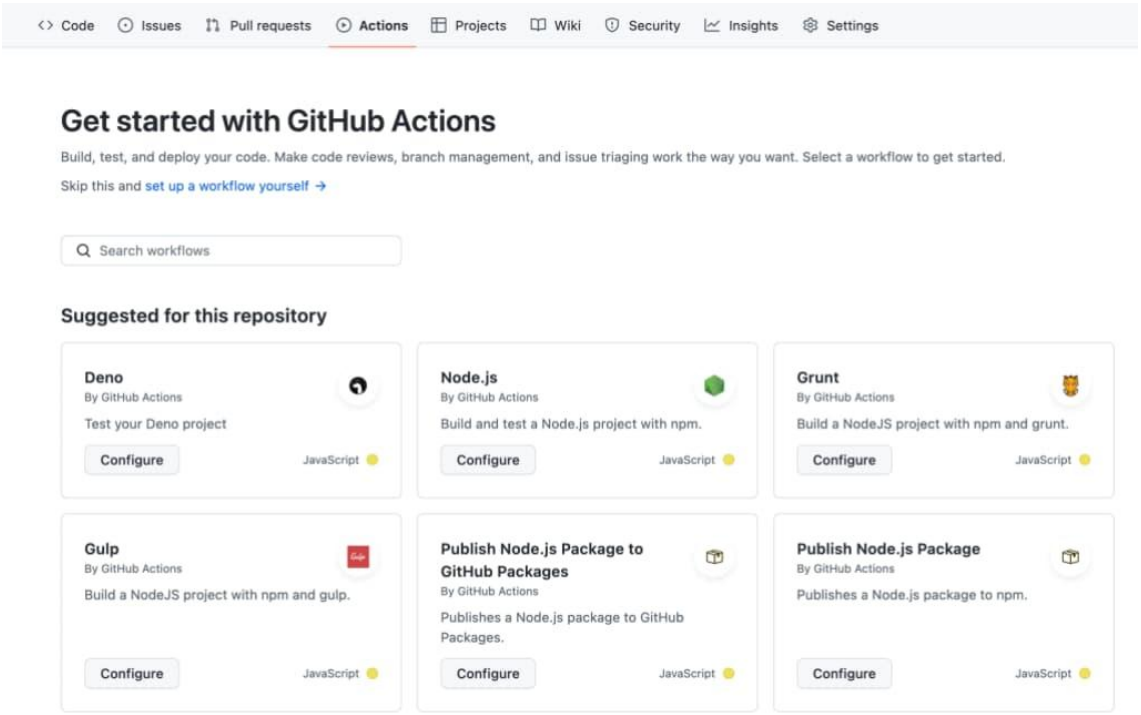
シームレスな開示プロセスにするために、GitHub Actionアドバイザリの作成時に以下の点を順守してください。

1. GitHub Actionでセマンティックバージョニングが使用されている。
2. アラートを作成しているアクションのリポジトリを所有している。
3. パッケージ名の形式を、"org-name/repo-name" (ユーザー名または組織名、スラッシュ、リポジトリ名)にする。例えば、"GitHub/GitHub's-favorite-action" のようになります。
4. 他のアクションと区別できるように、リポジトリ内のアクションを1つだけにする。

GitHub NEWS RELEASE

GitHub Actionsについて

GitHubリポジトリで最も使用されているCI/CDツールのGitHub Actionsは、あらゆる規模のチームが開発の迅速化と、ソフトウェアの信頼性向上を実現させます。再利用可能なワークフローとGitHub Actionsポリシー(組織または企業で使用できるアクションの制限など)を組み合わせて使用することで取り組みの範囲を拡大し、企業ならびに組織全体でより安全なコードベースを維持することを可能にします。既に作成済みの13,000個以上のActionsを選択し利用ができるため、誰でもGitHub Actionを使用して開発プロセスを改善できます。



GitHubサプライチェーンのセキュリティソリューションについて

GitHub Advisory Databaseによって公開されるセキュリティアドバイザリは、DependabotアラートやDependabotセキュリティアップデートといったGitHubサプライチェーンのセキュリティ機能の基盤となります。データはCreative Commonsライセンスによってライセンス供与されます。コミュニティはデータベース開始以降のすべてのデータを永久に無料で利用することができます。サプライチェーンのセキュリティ機能の詳細については、以下のページをご確認ください。

- GitHubで脆弱な依存関係を管理する方法
- GitHub Advisory Databaseへのアクセス

GitHub NEWS RELEASE

GitHub Blog
英語:
https://github.blog/2022-08-09-dependabot-now-alerts-for-vulnerable-github-actions/

日本語:
https://github.blog/jp/2022-08-26-dependabot-now-alerts-for-vulnerable-github-actions/

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は「開発者ファースト」の思想のもと、開発者のコラボレーションおよび困難な問題解決、世界にとって重要なテクノロジーの創出を促進させるための開発環境を提供しています。また、ソフトウェアを起点とする新たな未来を創造し、世界に変化をもたらすため、個人または企業規模に関わらず、ベストなコラボレーションができるコミュニティの拡大を支援しています。
安全なソフトウェア開発には、日常のワークフローの中でできる限り早いタイミングで脆弱性を発見し、対処できる仕組みづくりが重要です。GitHubは、企業とオープンソースのメンテナーが、ソフトウェア開発のライフサイクル全体を通じて、安全にコーディングできるようにするツールとプロセスを構築しています。
GitHubは、開発者がコードを開発、共有、そしてリリースする場です。学生や趣味で開発を行う人、コンサルタント、エンタープライズの開発者、経営者など、初心者から高い専門性をもつ世界8,300万人以上の方々および400万以上のOrganizationに利用されています。GitHubは単なるソースコードを共有する場ではありません。GitHubはオープンソースコラボレーションの源としてさまざまなソリューションを提供します。

【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