GitHub

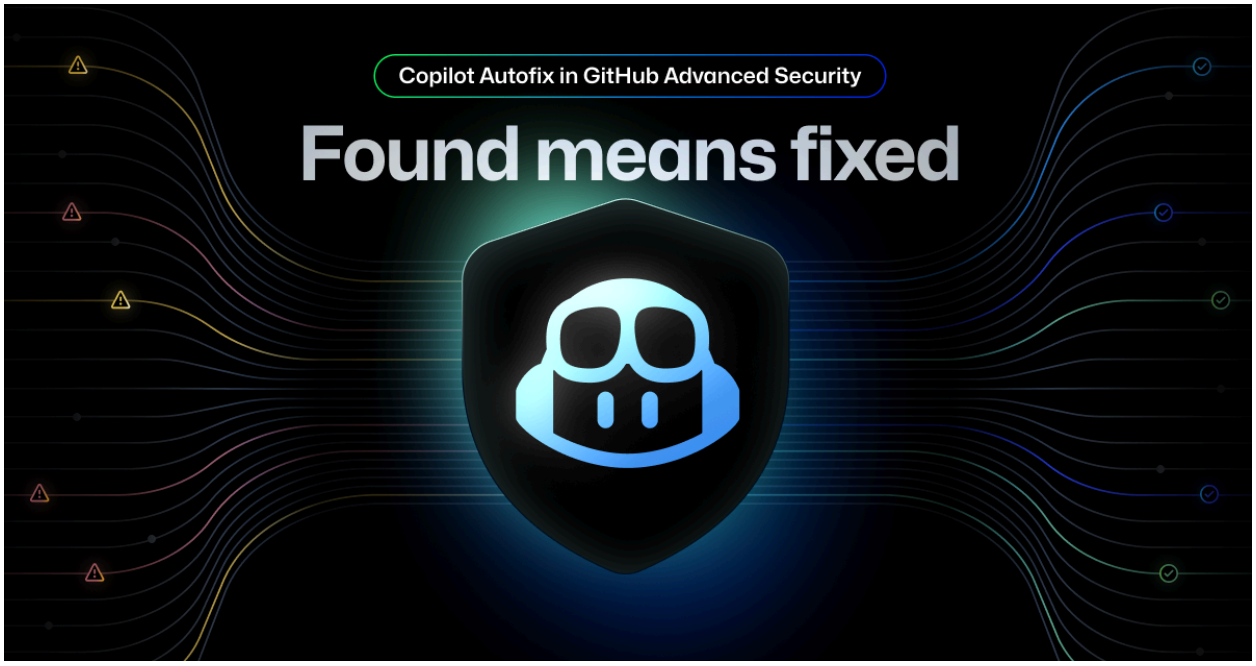
NEWS RELEASE

2024年8月15日
GitHub Japan

GitHub Copilot Autofix、脆弱性の発見と修正を同時に行い 3倍速くソースコードをセキュアにする新機能を発表

脆弱性が見つかることが修正されたことと同じ！

AIを活用したソフトウェア開発者プラットフォームとして世界をリードするGitHub, Inc.（本社：米国サンフランシスコ）は2024年8月14日(米国時間)、ソフトウェア開発者やセキュリティチームが新たな脆弱性をソースコードに持ち込むことなく、既存のセキュリティリスクを迅速かつ確実に修正できる新機能GitHub Copilot Autofix を発表しました。



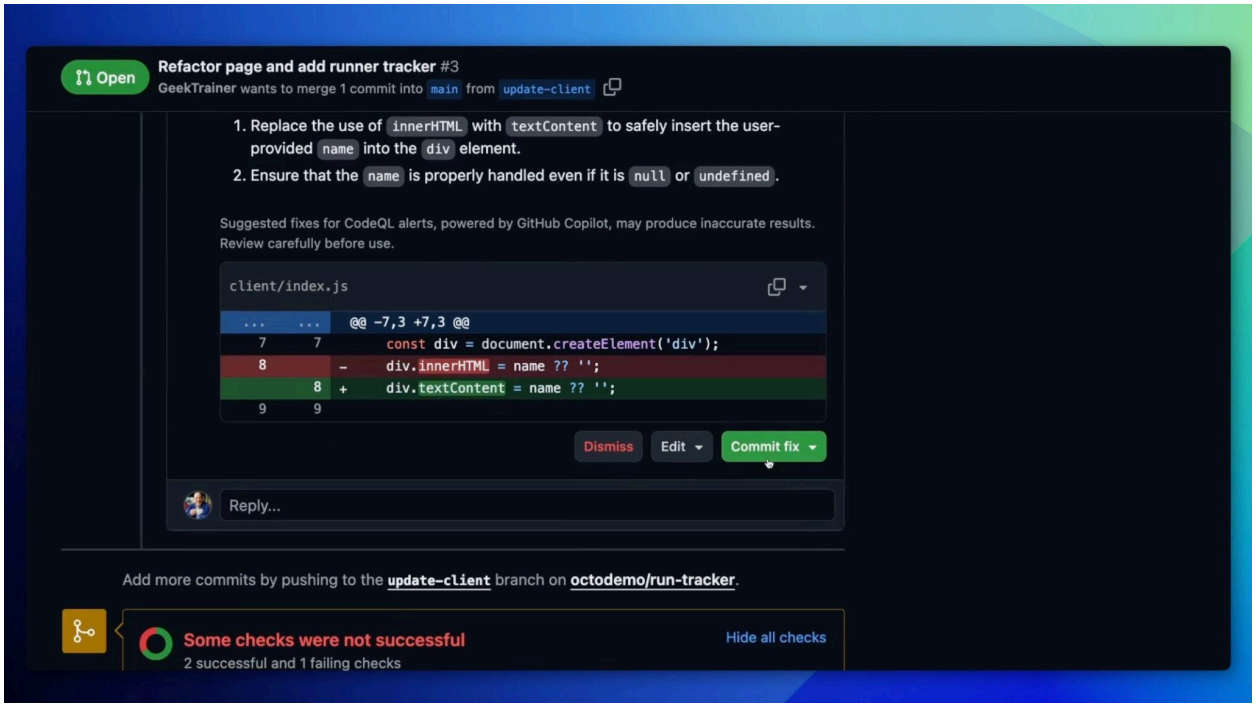
今日の開発者は、かつてない速さでソフトウェアをリリースし、新機能を早期かつ頻繁に提供しています。しかし、セキュアなソースコードを書くことに最善を尽くしても、ソフトウェアの脆弱性が意図せず開発中に入り込んでしまうことが、セキュリティ侵害の主な原因となっています。さらに、多くの開発者にとって、セキュリティの必須要件は理解しづらく、実装することが難しいため、セキュリティの観点から望ましい形になることが困難となっています。その結果、より多くの脆弱性が解決されないままリリースされてしまう状況に陥っています。

静的解析のツールは脆弱性を検出できますが、根本的な問題には対処できません。修復にはセキュリティの専門知識と時間が必要ですが、この貴重な2つの要素は決定的に不足しています。つまり、脆弱性を見つけることが問題ではなく、脆弱性を修正する行為が問題であると言えます。

このような状況を解決するための新たなアプローチとして、セキュリティ機能を拡張させるGitHub Advanced Security（GHAS）ライセンスに、AIがコード修正を支援する機能 GitHub Copilot Autofix を追加し、一般提供（GA）を開始しました。Copilot Autofix はコードに含まれる脆弱性を分析し、その重要性を説明するものです。加えて、脆弱性を発見するとすぐに開発者が修正できるようコードの提案を行います。パブリックベータ版のテストでは、開発者がコードの脆弱性を修正する際に、手作業で修正するよりも3倍以上速く修正できたことが判明しました。この結果は、AIエージェントがセキュアなソフトウェア開発を劇的に効率化させ、高速化できることを示す強力な事実となります。また、開発者は、Pull RequestでCopilot Autofix を使用し、コードから新たな脆弱性を排除し、既存の脆弱性を修正することで、既存のセキュリティ負債を削減することも可能になります。

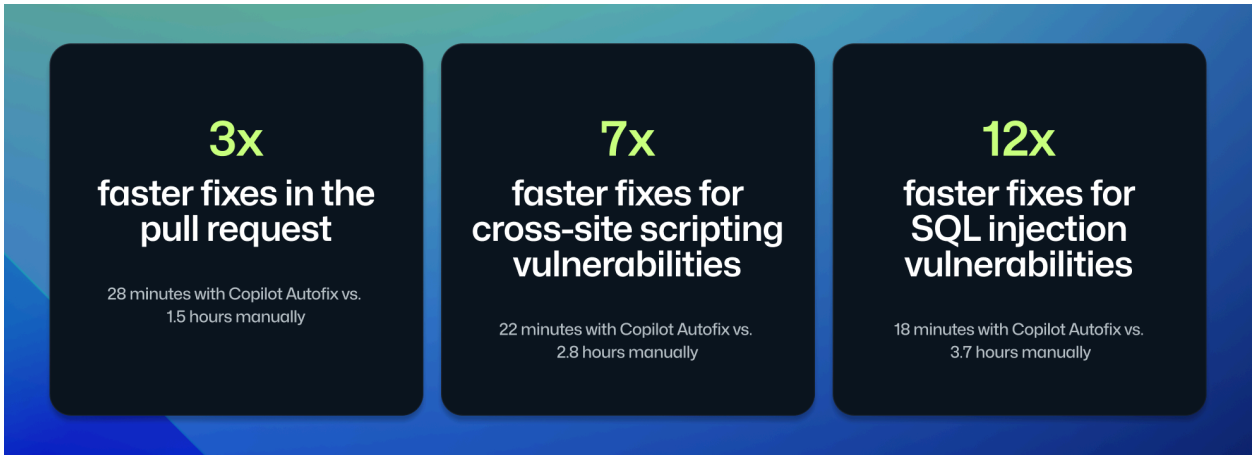
新しい脆弱性をコードから排除

2024年3月にパブリックベータ版として発表されて以降、開発者はPull RequestでCopilot Autofix を使用し、新しいコードの脆弱性を迅速に修正することで、製品コードにマージされることで顧客に影響を与えることを防止することができます。SQLインジェクションやクロスサイトスクリプティングなど、数十種類のコード脆弱性に対して修正が生成できるため、開発者はこれらの修正提案をPull Request内で却下、編集、またはコミットすることができます。



Pull RequestでのCopilot Autofixのデモ動画

2024年5月から7月までパブリックベータ版を利用したお客様のデータによると、Copilot Autofix は検出から修正までの時間を劇的に短縮しました。



*GitHub Advanced Security*を有効にしたリポジトリ上の*Pull Request*で*CodeQL*が新たに発見したコードスキャンアラートに基づいています。

- **3**倍速く：Pull Request時のアラート修正を自動コミットするまでの開発者の中央値は28分。手動で同じアラートを解決するのに1.5時間を要していたのに比べ、3倍速くなっています。
- **7**倍速く：クロスサイトスクリプティングの脆弱性は手動では約3時間かかっていましたが、22分で修正されました。
- **12**倍速く：SQLインジェクションの脆弱性は手動では3.7時間かかっていましたが、18分で修正されました。

Copilot Autofix のベータ版初期ユーザーからも、効率性と生産性の劇的な向上が報告されています。Optum社のプリンシパルエンジニアであるケビン・クーパー氏は、次のように述べています。「Copilot Autofix を導入してから、セキュリティ関連のコードレビューにかかる時間が60%削減され、開発生産性全体が25%向上しました。セキュリティが重要な医療分野において、業界で実証済みのソリューションを迅速に採用できるのは大きな利点です。このプロアクティブなセキュリティアプローチにより、潜在的な問題を未然に防ぎ、月に数千時間の修正作業を節約することができます」

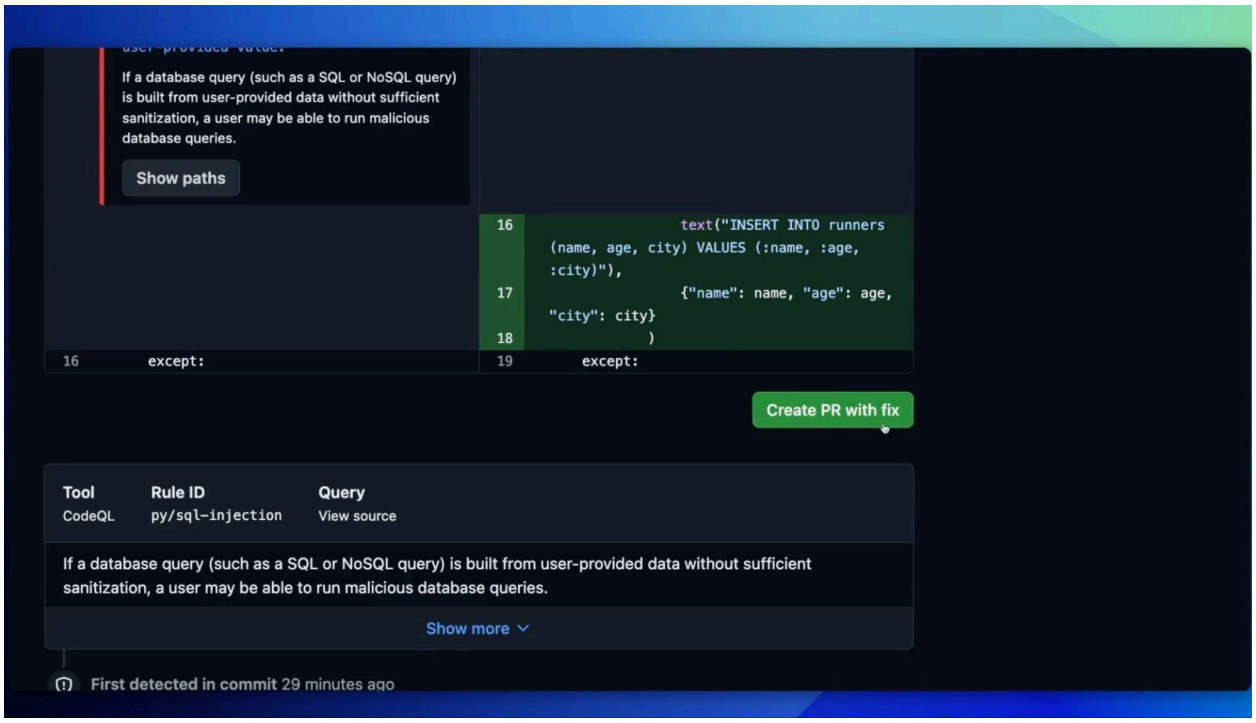
セキュリティ負債の削減

GitHub Copilotが開発者のコーディングを加速させるように、Copilot Autofixも修正のスピードを向上させ、セキュリティチームが既存の脆弱性、いわゆるセキュリティ負債の削減を進めることを可能にします。

脆弱性は放置していても無くなりません。放置していると修正が困難になりコストが増加してしまいます。ソフトウェア開発者がしばらく見ていないコードや馴染みのないコードの脆弱性を修正するように求められた場合、周囲のコードを評価し、手動で修正を試みる場合、数時間も要することがあります。Copilot Autofixはこの負担を大幅に軽減し、開発者が古い脆弱性をより迅速かつ確実に修正できるようにします。

使い方は簡単です。既存のコードの脆弱性に対してCopilot Autofix を起動するには、GHASのコードスキャンアラートで「Generate fix」ボタンを押すのみです。Copilot Autofix はコードと脆弱性を評価

し、レビュー用の説明とコード提案を返します。開発者はその後、「Create PR with fix」ボタンを押し、アラートを修正するコード変更を含む新しい Pull Request を作成できます。Copilot Autofix を使用すれば、優先順位付けが難しい低・中程度の脆弱性アラートを含め、数年間も蓄積されてきたセキュリティ負債を、わずか数クリックで解消できます。

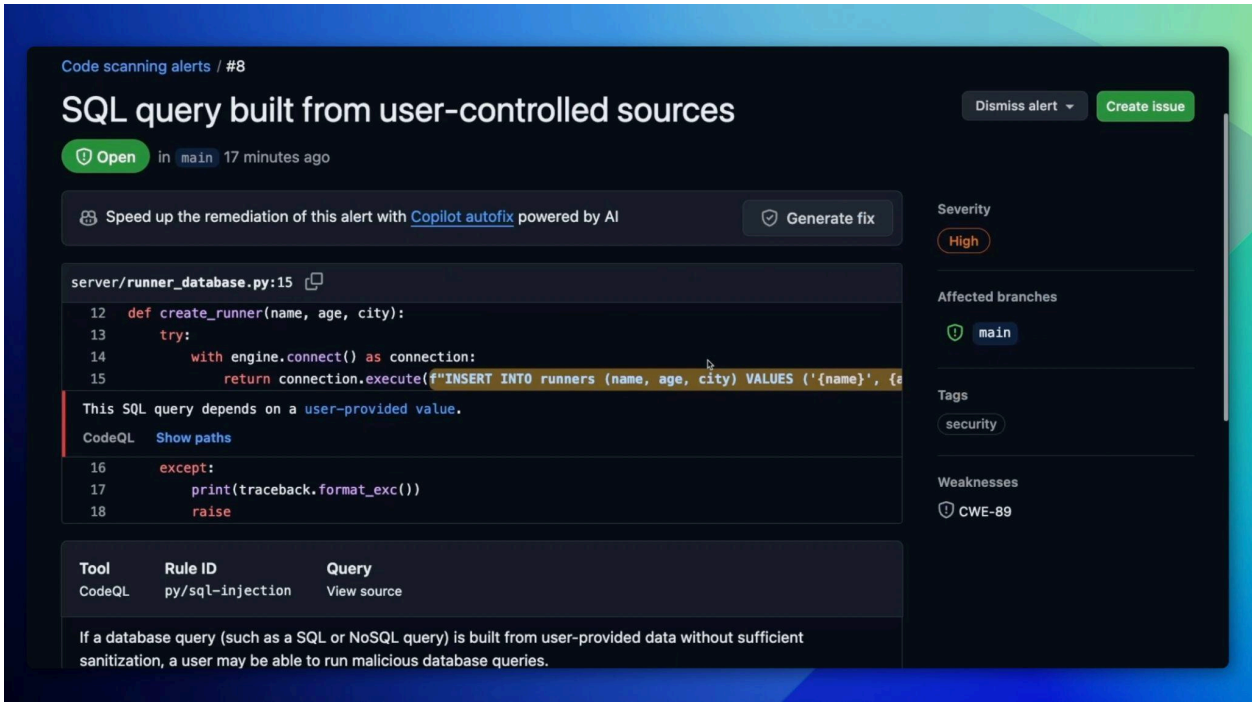


Copilot Autofix が既存のアラートの修正を生成するデモ動画

Otto（GmbH & Co KG）社のセキュリティ担当コミュニティマネージャ、マリオ・ランドグラフ氏は、「Copilot Autofixは、煩雑なセキュリティタスクを処理し、既存および新規のコードが可能な限り常にセキュアであることを保証してくれます。脆弱性を含むコードには直ちにフラグが立てられ、コードの変更が自動的に推奨されます。このおかげで、当社のチームは時間を自由に使えるようになり、より戦略的な取り組みに集中できるようになりました」とコメントしています。

Copilot Autofix の使用例

セキュリティの専門家ではない開発者にとって Copilot Autofix は、コードレビュー中にセキュリティチームの専門知識をすぐ手元に置いているかのような存在です。「*Copilot Autofix* は単に脆弱性にフラグをつけるだけではなく、特定のアクションが必要な理由とその実装方法を説明し、問題解決をより身近なものにしてくれます」とOptum社のクーパー氏は述べています。



動画を見る

Copilot Autofix の仕組みは、CodeQLエンジン、GPT-4o、および GitHub Copilot APIとヒューリスティックの組み合わせを活用し、コード提案を生成します。Copilot Autofixは、CodeQL分析とフローパス周辺のコードスニペットを含むソースに基づきLLMプロンプトを作成します。

GitHub Enterprise Cloud で GHAS をご利用のお客様は、デフォルトでCopilot Autofixが有効になっています。GHAS 製品にご興味のあるお客様は こちらからお問い合わせください。または、GitHub Japan営業およびサポート窓口（jp-sales@github.com）へお問い合わせください。

オープンソースのセキュリティを強化

Copilot Autofix は、プライベートリポジトリの脆弱性の修正に必要な時間と労力を削減するだけでなく、オープンソースの脆弱性にも対応が可能です。Log4j で見られたように、どこかに脆弱性があると、それがすぐにあらゆる場所へと拡大する可能性があります。GitHubは、オープンソースコミュニティのグローバルホームとして、メンテナーが脆弱性を検出し、修正することで、オープンソースソフトウェア（OSS）が誰にとっても、より安全で信頼性の高いものになるよう支援する唯一の場所となっています。GitHubは、オープンソースソフトウェアに関しては責任のある利用者であると同時に、そのコミュニティに貢献することが極めて重要であると強く信じています。そのため、オープンソースのメンテナーは、GitHubのコードスキャン、シークレットスキャン、依存関係管理、脆弱性非公開報告ツールを無料で提供しています。また、9月からは、Pull Request における Copilot Autofix をこのリストに加え、すべてのオープンソースプロジェクトへの無料提供を開始します。

迅速な対応と修正

ソフトウェアセキュリティの責任が引き続き開発者の肩に掛かっている一方で、AIエージェントがその負担を大いに軽減できると確信しています。熟練したセキュリティ人材が不足している状況であっても、Copilot Autofix を使用することで、すべての開発者が必要なときにセキュリティの専門知識を享受できます。セキュリティは、ソフトウェア開発と同義のものとなるのです。

今回、新機能を提供したばかりですが、GitHub Copilot Workspace からGHASに至るまで、GitHubは単にAIで支援するだけではなく、生産性やイノベーションからセキュリティ、リスク軽減に至るまで、ビジネスを変革する未来を目指しています。GHASでは、AIを活用してコードの脆弱性を修正するだけでなく、シークレットスキャンの範囲と精度を向上させ、新たなワークフローで大量のセキュリティ負債を抱える組織にも対応できるようにするために、すべての開発者が慣れ親しんでいるプラットフォーム上で実現しています。

Copilot Autofixにより、”Found means fixed”（脆弱性が見つかることが修正されたことと同じ意味を持つ）というビジョンに一歩近づきました。

GitHub Blog
英語:
https://github.blog/news-insights/product-news/secure-code-more-than-three-times-faster-with-copilot-autofix/

日本語:
https://github.blog/jp/2024-08-15-secure-code-more-than-three-times-faster-with-copilot-autofix/

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
X: (英語) @github https://twitter.com/github
(日本語) @GitHubJapan https://twitter.com/githubjapan

【GitHub について】
GitHubは、すべての開発者のためのグローバルなホーム(家)として、安全なソフトウェアの開発、拡張、提供を実現に向け世界有数のAI搭載開発者プラットフォームです。『Fortune 100』(グローバル企業の総収入ランキングトップ100)に名を連ねる90社の開発者を含む1億人以上の人々がGitHubを利用し、4億2,000万以上のリポジトリで素晴らしい共同作業を行っています。GitHubが提供するあらゆるコラボレーション機能により、個人やチームはかつてないほど容易に、より速く、より良いコーディングを実現しています。
GitHub.com (日本語サイト https://github.co.jp)

【製品／サービスに関するお問い合わせ先】
GitHub Japan営業およびサポート窓口
Email: jp-sales@github.com