GitHub

NEWS RELEASE

2022年6月2日
ギットハブ・ジャパン合同会社

GitHub、8周年を迎えたセキュリティバグ報奨金プログラム

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、5月23日（米国時間）に、2021年GitHubのセキュリティバグ報奨金プログラムが、再びこれまでの記録を塗り替え、研究者への支払い総額が2,000,000米ドルを超えたことを発表しました。

セキュリティバグ報奨金プログラムは、GitHub、GitHubの製品、開発者コミュニティ、GitHubの顧客のセキュリティを高めるために導入されており、研究者への支払い総額が2019年に1,000,000米ドルを超えてからわずか2年、2021年にこれまでの記録を再び塗り替え、2,000,000米ドルを超えました。昨年1年間では、プログラム全体で合計800,000米ドル以上の報奨金が支払われました。セキュリティバグ報奨金プログラムの成功を支えた基盤は、コミュニティ全体の有能なセキュリティ研究者とのパートナーシップがあったからこそ実現できたものであると確信しています。

セキュリティは、GitHubが掲げるミッションの中核を成すものであり、昨年、GitHubはバグ報奨金プログラムの実施と発展を専門とする新しい社内チームの発足を発表しました。コミュニティの関与、運用、プログラムの発展に重点的に取り組むこのチームを当社のProduct Security Engineering部門に迎え入れることは、報奨金プログラムの継続的な発展と成熟にとって欠かせないものでした。

昨年1年間に報奨金コミュニティと一緒に成し遂げた、いくつかの成果をご紹介します。2022年後半の展望と、今年6月に開催予定のHackerOneとのライブハッキングイベントについては下記をご確認ください。

2021年のハイライト
専門のバグ報奨金チームが発足してから10か月で、2021年の記録を上回りました。2021年2月から2022年2月までの主要なハイライトは以下のとおりです。

- 235個の脆弱性に対する報奨金として、803,769米ドルが支払われました。2016年以降にHackerOneを通じて支払った報奨金の総額は2,355,773米ドルとなりました。
- 公開プログラムと非公開プログラム全体で、1,363件の報告がありました。2022年1月が最も多く、報告数は149件でした。
- 2021年11月には、1件の報奨金として史上最高額の50,000米ドルが支払われました。
- 研究者からの報奨金の寄付額が64,000米ドルを超え、合計で128,234米ドルがさまざまな慈善事業に寄付されました(寄付プログラムの詳細については、こちらをご覧ください)。
- 回答時間が2020年から1時間改善し、最初の回答までが平均12時間となりました。
- プログラムへのコントリビュータが21%増加し、初回レポートが18%増加しました。

GitHub NEWS RELEASE

2021年に**GitHub**で話題となったバグ
2021年に寄せられた報告の中から、特に興味深かったものに関して詳しくご紹介します。

パストラバーサル
2021年7月2日、GitHub Enterprise Server (GHES)にパストラバーサルの脆弱性について報告がありました。

GHESのパストラバーサルの脆弱性は、GitHub Pagesサイトの構築時に発生しました。GitHub Pagesを使用すると、ユーザーは一連の構成オプションによってサイトをパーソナライズできます。このようなユーザー制御の構成オプションに対する制限が不十分であったため、攻撃者はパストラバーサルを利用してGHESインスタンス上のファイルを読み取ることができました。攻撃者がこの脆弱性を悪用するためには、GHESインスタンス上にGitHub Pagesサイトを作成および構築するための権限が必要でした。

GitHubはこの問題を修正し、CVE-2021-22867およびCVE-2021-22868を割り当てました。CVE-2021-22867の修正プログラムには、異なるペイロードを使用すれば引き続きパストラバーサルが可能であるという回避策が見つかったため、CVE-2021-22868が発行されました。

この脆弱性は、3.1.8より前の全バージョンのGitHub Enterprise Serverに影響を及ぼし、3.1.8、3.0.16、および2.22.22で修正されました。

研究者のyvvdwfは、非常に有意義な発見を最初に報告しただけでなく、修正プログラムが利用可能になるとそのテストを支援し、このテストとバリアント分析により、初期修正プログラムの回避策を見つけることもでき、最終的に、この発見によって製品のセキュリティをさらに高めることができました。こうした継続的な取り組みを評価し、GitHubはテスト支援に関してyvvdwfにボーナスを支給し、追加の発見に関しては別の報奨金を提供しました。

研究者スポットライト
2021年10月、GitHubはプログラムに参加している研究者数名に焦点を当てて、サイバーセキュリティ啓発月間を実施しました。このようにスポットライトを当てることにより、GitHubのプログラムに参加している研究者について深く理解する機会となっただけでなく、彼らがGitHubやその他のバグ報奨金プログラムにもたらすユニークな才能や専門知識を幅広く紹介できる絶好の機会ともなりました。今年の研究者のハイライトは、下記のサイトからご確認ください。

- Cybersecurity spotlight on bug bounty researcher @yvvdwf
- Cybersecurity spotlight on bug bounty researchers @chen-robert and @ginkoid

今後の展望
GitHubの製品およびサービスの拡大と発展に合わせて、今後も報奨金の対象範囲に新たな重点分野を追加していく予定です。たとえば、今年は、非公開の報奨金プログラムに製品を取り入れた後、対象範囲にnpmを追加しました。このプログラムは成功を収め、3つの重大な脆弱性の発見につながりました。また、総合的なセキュリティ投資の一環として、今後も重点分野を絞った非公開の報奨金プログラムへの投資を続けていきます。

さらに、プログラムに参加している研究者を奨励するための、新たな方法を検討しています。金銭的な報酬に加えて、支払い基準を満たしていないレポートを評価するために、金銭以外の報酬を導入することにも注力しています。研究者の尽力に報いる方法はたくさんあり、金銭や表彰など、さまざまな研究者のモチベーションに合わせて異なる報酬を用意することで、引き続き研究者とのより良い関係を築き、彼らの取り組みを評価することができるでしょう。

2022年6月には、HackerOneとのライブハッキングイベントを開催します。GitHubは、コミュニティの人々と共に時間を過ごすことに非常に大きな価値を見いだしており、GitHubに焦点を当てた最初のイベントを開催できることを嬉しく思っています。ここ数か月間はHackerOneと連携して、会場に来られる参加者とリモート参加者のどちらにも楽しんでいただけるようなイベントを計画してきました。イベントへのアクセスは制限されていますが、下記より今後のライブハッキングイベントへの参加方法をご確認いただけます。https://www.hackerone.com/live-hacking-events

GitHubのバグ報奨金プログラムは9年目になりました。今後もプログラムを改善し、研究者やエンジニアに最高のエクスペリエンスを提供できるようにしていく予定です。2023年は、回答時間の改善、ハッカーコミュニティへの参加、継続的なレビュー、研究者を対象とした魅力的な報酬に関して情報を発信していきます。

プログラムの対象範囲、ルール、報酬の詳細については、GitHubのウェブサイトをご確認ください。

GitHub Blog
英語:
https://github.blog/2022-05-23-eight-years-of-the-github-security-bug-bounty-program/

日本語:
https://github.blog/jp/2022-05-31-2022-05-23-eight-years-of-the-github-security-bug-bounty-program/

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 NEWS RELEASE

【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