GitHub

NEWS RELEASE

2021 年 7 月 15 日
ギットハブ・ジャパン合同会社

7 周年を迎えた
GitHub 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、6 月 25 日（米国現地時間）に 7 周年を迎えた GitHub セキュリティバグ報奨金プログラムのハイライトおよび今後の展望を公開しました。

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す。GitHub の Product Security Engineering チームは、GitHub を使って安全なソフトウェアを開発する方法の継続的な改善に取り組んでいます。GitHub が取り組むセキュリティの開発ライフサイクルにおいて重要な要素の 1 つが、GitHub セキュリティバグ報奨金プログラムを通じたセキュリティ研究者やバグ報奨金コミュニティとのパートナーシップです。2014 年のプログラム開始以来、このプログラムと研究者たちの貢献によって、GitHub はより安全な製品を提供することができるようになりました。これらは、GitHub のチームだけでは実現が難しいものです。今年で 7 年目となるバグ報奨金プログラムは、GitHub による製品セキュリティの継続的な向上を可能にする、成熟した信頼できる要素となっています。

セキュリティバグ報奨金プログラムによって軽減された興味深い脆弱性の詳細や来年に向けた展望を紹介します。拡大を続けるバグ報奨金プログラムへのコミュニティの皆さまのご参加を心よりお待ちしています。

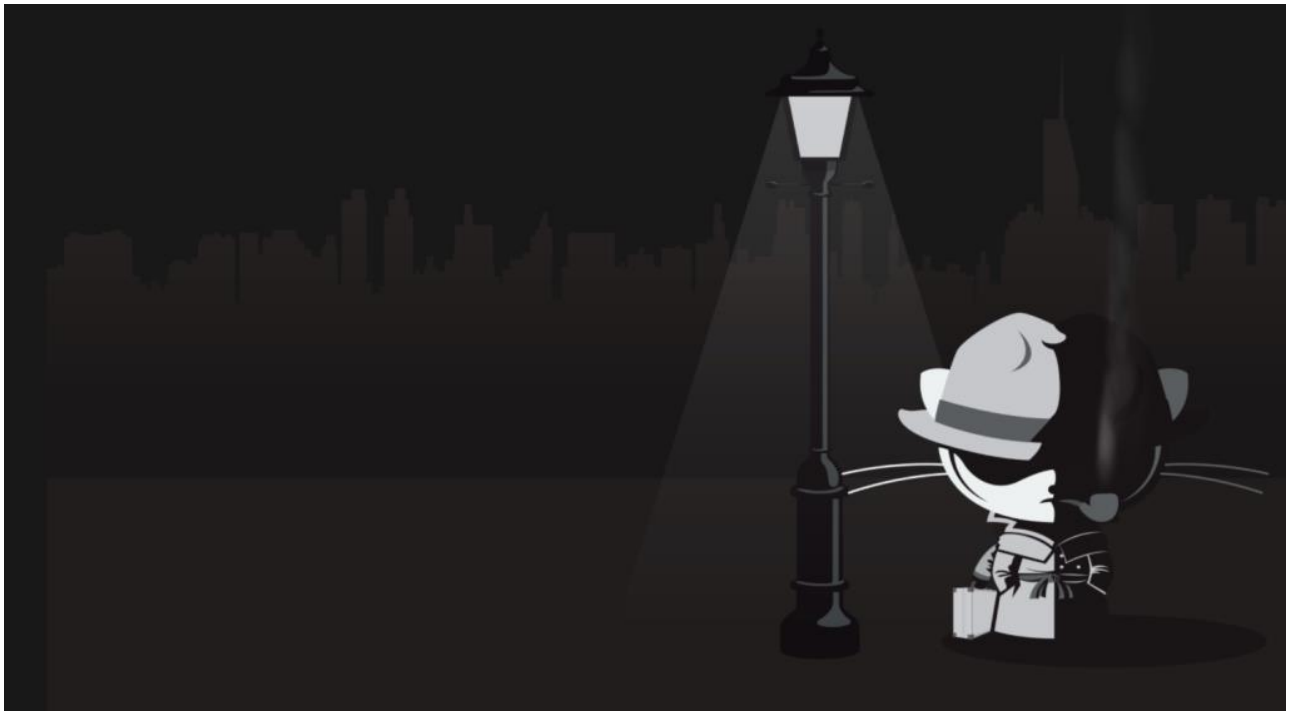
2020 年のハイライト

2020 年はこれまでで最も忙しい年となり、同年 2 月から 2021 年 2 月までの間に、過去最多のセキュリティバグ報告に対応しました。本プログラムが拡大を続ける中、バグ報告への最初の返信、トリアージ、支払いまでの時間について、挑戦的な基準を維持してきたことは GitHub の誇りとなっています。昨年のハイライトを以下にご紹介します。

- GitHub の製品やサービスで見つかった 203 件の脆弱性に対し、524,250 米ドルの報奨金が支払われました。その結果、2016 年に HackerOne に移行してからのプログラム全体の報奨金は 1,552,004 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、1,066 件の報告がありました。
- 回答時間は 2019 年から 4 時間の改善に成功し、最初の回答までが平均 13 時間となりました。
- 報告されたものは、平均 24 時間以内に社内で検証され、パートナーチームにトリアージされました。
- 報奨金は、対象となる報告が行われてから平均 24 日後に支払われました。
- GitHub のプログラムが、HackerOne のトッププログラムの 1 つにランク付けされました

バグ報奨金プログラムへの報告は、GitHub、GitHub の製品、開発者コミュニティ、ならびに GitHub のお客様のセキュリティを高度化させる機会に貢献します。オープンソースコミュニティの方々のスキルをお借りして、すべての人にとって GitHub をより良いものにしていくための継続的なコラボレーションに期待が寄せられています。本プログラムへの参加にご興味のある方は、プログラムの対象範囲、規則、報奨金などの詳細はウェブサイトをご確認ください。



2020 年に GitHub で話題となったバグ

GitHub の報奨金プログラムに寄せられるバグ報告の創造性と深い技術的才能には、当社はいつも感心させられています。その一例として、特に興味深かったものについて詳しくご紹介します。

GitHub NEWS RELEASE

ユニバーサルオープンリダイレクト (Universal open redirect)

オープンリダイレクト単独では通常、ソーシャルエンジニアリング攻撃の足掛かりにしかならないため、オープンリダイレクトの脆弱性が、アプリケーションに深刻な影響やリスクをもたらすことは稀です。しかし、William Bowling 氏 (@vakzz)は、GitHub.com のオープンリダイレクトの脆弱性を利用して、Gist ユーザーの OAuth フローを侵害する方法を示すことに成功しました。

William 氏は、GitHub.com の多数のコントローラで使われているメソッドが、Ruby on Rails の”url_for”ルーティングメソッドに、リンクやリダイレクト先を生成する安全ではないユーザー制御の引数を与えていることを発見しました。JavaScript プロトコルハンドラーを与えると、クロスサイトスクリプティング (XSS)が生じる可能性がありましたが、GitHub.com には強力なコンテンツセキュリティポリシーがあるため、潜在的な XSS のリスクは軽減されます。ただし、この生成された URL はリダイレクト先として使われていたため、攻撃者が選択した場所にユーザーをリダイレクトする目的で使われる可能性がありました。リスクはかなり低いのですが、この脆弱性を利用して、提供した GitHub.com へのリンクから最終的には攻撃者が指示するサイトにリダイレクトさせることで、ソーシャルエンジニアリング攻撃を容易にすることができました。

William 氏は、GitHub のリクエストハンドラーでこの脆弱なメソッドが広く使われていることを考慮し、このバグの影響をさらに踏み込んで調査しました。このリダイレクトを、GitHub.com が GitHub Gist の認証を実行する OAuth フローと組み合わせて利用することにより、OAuth 認証が成功した後でユーザーをリダイレクトし、ユーザーの OAuth コードを攻撃者が決めた場所に流出させることができました。その結果、攻撃者は、悪意のあるリンクに騙されたユーザーの GitHub Gist にログインできるようになります。

GitHub では、内部的に”safe_url_for”および”safe_redirect_to”というヘルパーメソッドが用意されているため、信頼できないリダイレクト先やプロトコル、その他の危険な引数をフィルタリングすることで、このような種類の脆弱性を防いでいます。オープンリダイレクトの脆弱性を軽減するために、脆弱性のあるコードをリファクタリングし、安全なバリアントを使用して、”url_for”に対する特定の引数をユーザーが制御できないようにしました。さらに、継続的に実行しているスタティック分析ツールにチェック機能を追加し、ユーザー制御の引数を持つ新しいコードに”url_for”が追加されたことが検出できるようにしました。このように、この種の脆弱性を捕捉する安全策を講じることにより、コードベース全体でこのクラスの脆弱性の排除を進めました。

この報告には 1 万米ドルの報奨金が支払われました。オープンリダイレクトが他の機能と連係した場合の影響を実証するために調査を続けた William さんの粘り強さに感謝しています。この脆弱性の詳細については、William 氏のブログをご覧ください。

CVE の発行

昨年のバグ報奨金プログラム 6 周年ニュースリリースでお伝えしたとおり、2020 年に GitHub は MITRE の CVE 採番機関(CNA)となり、GitHub Enterprise Server の脆弱性に対する CVE の発行を開始しました。CNA になったことで、製品で修正された問題を明確かつ一貫してお客様に伝えることができるようになり、お客様は古くなった GitHub Enterprise Server インスタンスを適切に識別し、アップグレードの優先順位を決められるようになりました。さらに、バグ報奨金プログラムに報告された GitHub Enterprise Server の脆弱性はその CVE の研究者の功績となるため、GitHub のプログラムに参加している研究者の評価をさらに高めることができます。

このプロセスを支援するため、GitHub は CVE 発行の社内ワークフローを形式化しました。脆弱性を GitHub の問題として社内で追跡する手段と連動する自動化を行い、CVE の詳細が明確で一貫したものになるよう、以下のように手順を標準化しました。

- chat-op を実行し、GitHub 製品のすべての脆弱性に対して発行される社内の脆弱性追跡番号に基づき、新しい Pull Request を作成します。
- Product Security Engineering チームのメンバーが、説明、カテゴリー、重大度、修正バージョンなどのすべての詳細情報を、Markdown テンプレートに入力します。
- Product Security Engineering チームの他のメンバーやエンジニアリングチームがこれをレビューし、Pull Request 内でフィードバックを提供します。
- 公開の準備が整ったら、GitHub Actions によってこれを MITRE が使用する JSON 形式に変換し、”CVEProject/cvelist”リポジトリに追加できるようにします。

昨年、GitHub はこのワークフローとツールの改良を続け、GitHub Enterprise Server の CVE を 3 件公開しました。2021 年に入ってからもこのワークフローは効果的に機能していることから、7 件の追加アドバイザリの CVE プロセスを迅速に完了させることができました。より多くの CVE と製品の修正に役立つ詳細を提供できれば、GitHub Enterprise Server のお客様にアップグレードの優先度をより簡単に伝えることができます。

非公開のバグ報奨金

2020 年、GitHub は公開されているバグ報奨金プログラムに加えて、ベータ版などのプレリリース製品を対象とした非公開のバグ報奨金プログラムの取り組みを開始しました。非公開の報奨金プログラムは、新製品や新機能のソフトウェア開発ライフサイクルの早い段階で問題を特定し、開発の後半になってからで

は困難となるアーキテクチャや設計の変更をより容易に展開できるようにします。

GitHub Pages の非公開表示

2020 年の非公開バグ報奨金プログラムでは、GitHub Pages の表示制限に焦点が当て取り組みました。従来は、GitHub Pages を公開すると、インターネット上に公開されていましたが、このたびの新機能では、基盤となるリポジトリにアクセスできる GitHub ユーザーのみにアクセスを制限できます。これは社内ドキュメントサイトやポータルを作成できる素晴らしい機能ですが、GitHub Pages を実装するために複雑なアーキテクチャの変更を必要としていました。このような複雑さにはリスクが付き物であるため、Product Security Engineering チームは GitHub のエンジニアと協力し、GitHub Pages の認証プロセスを設計し、社内のセキュリティテストとコードレビューを通じて実装を検証しました。

また、さらなる保証のために、この機能を非公開のバグ報奨金プログラムの対象とし、2020 年 5 月から参加ている研究者に、開発中のこの機能への早期アクセスを許可しました。Robert Chen 氏(@notdeghost)と Philip Papurt 氏(@ginkoid)の 2 人の研究者は、XSS とその他いくつかの脆弱性を組み合わせることで、GitHub Page の表示設定を回避できることを特定しました。この 2 人の研究者には、特定した脆弱性に対してだけでなく、報奨金の一部として設定した旗取り合戦(Flag Challenge)を成功させたことに対して、35,000 米ドルの報奨金が支払われました。GitHub は、この機能をリリースする前に特定された問題を修正し、今後同様の脆弱性に対してもこのサービスがより強固なものになるよう、アーキテクチャを強化することができました。

GitHub Enterprise Server 2.22

2020 年にはまた、非公開のバグ報奨金プログラムの研究者に GitHub Enterprise Server 2.22 を早期公開しました。これは、コンテナベースの新しいアーキテクチャを採用した初めての GitHub Enterprise Server のリリースであり、GitHub Actions、GitHub Packages、GitHub Advanced Security に含まれる Code Scanning をベータ機能として追加した初めてのリリースでもありました。こうした新機能に加えて新たなアーキテクチャを採用したため、GitHub はセキュリティ開発ライフサイクルにこの特別なレビューステップを追加したいと考えたのです。

GitHub Codespaces

今年は、新機能や新製品の早期リリースを確実にするため、非公開プログラムの拡充に引き続き力を入れています。6 月には、GitHub Codespaces を対象とした新しい非公開の報奨金プログラムを開始しました。GitHub Codespaces は、クラウド上に完全な開発環境を提供するだけでなく、独自のアーキテクチャとセ

キュリティ対策が施されています。この非公開のバグ報奨金プログラムでは、このサービスを安全な方法で設計、実装する内部作業を検証するために、研究者の参加を認めています。現在、この非公開プログラムに参加してくださっている皆さまの多大なる貢献に感謝しています。

今後の展望

2021 年には GitHub のセキュリティプログラムへの大きな投資と発展がありました。6 月には、バグ報奨金プログラムの実施と発展を専門とする、新しい社内チームが発足しました。GitHub のプログラムに参加している皆さまは、セキュリティバグの報告の向こう側にいる新たなメンバーにぜひ期待してください！このチームは、トリアージプロセスと回答プロセスをさらに加速させ、改良にも取り組み、ライブハッキングイベントやさらなる非公開のバグ報奨金プログラムなど、新たな展開を拡大していきます。

バグ報奨金プログラムのアニバーサリーを迎えるにあたり、プログラムに参加してくださっている研究者の皆さまに改めて感謝の意を表すと共に、次の 1 年の活動に期待を寄せています。セキュリティへの継続的な投資の一環として、GitHub は Product Security Engineering チームとより広範な GitHub のセキュリティ組織を拡大しています。GitHub がバグ報奨金プログラムや開発ライフサイクルを通じて行っている、製品やサービスのセキュリティ対策に興味をお持ちの方は、https://github.com/about/careers で募集中の職種をご確認ください。

GitHub Blog
英語 https://github.blog/2021-06-25-seven-years-github-security-bug-bounty-program/

日本語
https://github.blog/jp/2021-07-15-seven-years-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 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