PRESS RELEASE

2025 年 1 月 27 日

報道関係各位

GMO Flatt Security 株式会社

GMO Flatt Security の RyotaK が Git の認証情報漏洩につながる 6 個の脆弱性を Git および GitHub 関連サービスに報告

GMO インターネットグループでプロダクト開発組織に向けたサイバーセキュリティ関連事業を展開する GMO Flatt Security 株式会社（代表取締役社長：井手 康貴　以下、GMO Flatt Security）の「脆弱性リサーチプロジェクト」において、セキュリティリサーチャーの RyotaK が Git の認証情報漏洩につながる 6 個の脆弱性を報告しました。

関連するプログラム・サービスをご利用の皆様はアドバイザリに従いアップデート等の対策を実施することを推奨いたします。

【「脆弱性リサーチプロジェクト」とは】

GMO Flatt Security はソフトウェアプロダクトの脆弱性診断を主軸としてサービスを展開しており、脆弱性の検出において世界トップクラスの実力を持つエンジニアが複数在籍しています。その高い脆弱性検出能力を活かして始まった取り組みが GMO Flatt Security の「脆弱性リサーチプロジェクト」です。日々の脆弱性診断サービス提供の枠組みの外でも、社会を支える種々のシステムのセキュリティを調査・脆弱性を報告し、その過程で得られた知見を日本発でグローバルに発信しています。

■「脆弱性リサーチプロジェクト」の成果など、グローバルな技術発信を行う英語ブログ

・「GMO Flatt Security Research」　https://flatt.tech/research/

■「脆弱性リサーチプロジェクト」の成果のうち開示済みの CVE 一覧

https://flatt.tech/cve

■「脆弱性リサーチプロジェクト」の過去の実績

・執行役員・志賀が Ubuntu の権限昇格の脆弱性を報告し、世界最大級のハッキングコンテスト「Pwn2Own」で 3 万 US ドルの報奨金を獲得。
https://scan.netsecurity.ne.jp/article/2021/05/27/45729.html

・セキュリティリサーチャー・RyotaK が Windows においてコマンドインジェクションを引き起こすことができる脆弱性を Java・PHP・Ruby・Go など 8 の言語に対して報告。
https://flatt.tech/research/posts/batbadbut-you-cant-securely-execute-commands-on-windows/

【今回報告した脆弱性】

今回、GMO Flatt Security の RyotaK は Git や GitHub 関連サービスに対して以下の 6 個の脆弱性を報告しました。複数の脆弱性の組み合わせによって、最終的に Git の認証情報が悪意のある攻撃者に窃取されてしまう可能性があります。Git の認証情報が窃取されるということは、多くのソフトウェア企業において最も重要な資産であるソースコードが外部に流出したり、本番環境のソースコードに悪意のあるプログラムが混入させられてエンドユーザーに被害が及んだりするリスクがあることを意味します。

Git および GitHub は世界中の開発者に利用されているプログラムであり、今回適切なフローで開発元に報告し、アドバイザリが開示されたことで世界の安全に資することができました。

なお、GitHub Codespaces の脆弱性以外はユーザー側での対策が必要です。関連するプログラム・サービスをご利用の皆様はアドバイザリに従いアップデート等の対策を実施することを推奨いたします。

今回報告した脆弱性に関する詳細な解説は下記の英語ブログ記事で公開しています。
https://flatt.tech/research/posts/clone2leak-your-git-credentials-belong-to-us/

■CVE-2024-52006

Git における、クレデンシャルヘルパーに対してキャリッジリターンを送信してしまう問題

■CVE-2025-23040

GitHub Desktop においてキャリッジリターンの取り扱いが不適切であるため、CVE-2024-52006 と組み合わせることで Git の認証情報が漏洩する問題

■CVE-2024-50338

Git Credential Manager においてキャリッジリターンの取り扱いが不適切であるため、CVE-2024-52006 と組み合わせることで Git の認証情報が漏洩する問題

■CVE-2024-53263

Git LFS において、クレデンシャルヘルパーに対して改行文字を送信してしまい、Git の認証情報が漏洩する問題

■CVE-2024-53858

GitHub CLI を GitHub Codespaces 上で実行した際、任意のホストに対して GitHub.com 用のアクセストークンを送信してしまう問題

■GitHub Codespaces の脆弱性（ユーザー側での対策が不要なので CVE 採番なし）

GitHub Codespaces 上に実装されているクレデンシャルヘルパーにおいて、ホスト名検証が行われていないため、認証情報が外部のホストに対して送信されてしまう問題

【GMO Flatt Security 株式会社について】

GMO Flatt Security は「エンジニアの背中を預かる」をミッションに、業界を問わず DX 推進・ソフトウェア開発のセキュリティを支援してきた、日本発のセキュリティプロフェッショナル企業です。セキュリティ製品の自社開発や様々な企業へのセキュリティ支援、徹底したユーザーヒアリングを通じて得た知見を元に、一つひとつの顧客組織に寄り添った伴走型のセキュリティサービスを提供しています。

■「エンジニアの背中を預かる」ための、エンジニア向けサービス群

・Web&クラウドまるごと脆弱性診断ツール「Shisho Cloud byGMO」
URL： https://shisho.dev/ja
・セキュリティエンジニアによる手動脆弱性調査・分析サービス「脆弱性診断」
URL：https://flatt.tech/assessment
・クラウド型セキュアコーディング学習プラットフォーム「KENRO byGMO」
URL： https://flatt.tech/kenro

株式会社 Flatt Security は 2025 年 1 月 20 日より、GMO Flatt Security 株式会社に社名を変更いたしました。

以上

【報道関係お問い合わせ先】

●株式会社 GMO Flatt Security　広報
E-mail：pr@flatt.tech

●GMO インターネットグループ株式会社
グループ広報部　PR チーム　田部井
TEL：03-5456-2695
お問い合わせ：https://www.gmo.jp/contact/press-inquiries/

【GMO Flatt Security 株式会社】（URL：https://flatt.tech）

会社名	GMO Flatt Security 株式会社
所在地	東京都渋谷区桜丘町 26 番 1 号 セルリアンタワー
代表者	代表取締役社長　井手 康貴
事業内容	■サイバーセキュリティ関連サービス
資本金	4 億 3,042 万円（資本準備金含む）

【GMO インターネットグループ株式会社】（URL：https://www.gmo.jp/）

会社名	GMO インターネットグループ株式会社　（東証プライム市場　証券コード：9449）
所在地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代表者	代表取締役グループ代表　熊谷 正寿
事業内容	■インターネットインフラ事業　■インターネット広告・メディア事業 ■インターネット金融事業　■暗号資産事業
資本金	50 億円