



緊急報告: GitLabアカウント 乗っ取りの危機

本日、弊社が利用するGitLabに、認証なしでアカウントを乗っ取ることが可能な**極めて深刻な脆弱性**が存在することが確認されました。

この問題は、弊社の知的財産、開発プロセス、そして事業継続そのものに直接的な脅威をもたらします。

本報告の目的は、この危機的状況を回避するため、**経営層による迅速なご判断とご承認**をいただくことです。

問題の特定と客観的な深刻度

発見された脆弱性は、パスワードリセット機能の致命的な欠陥に起因します。攻撃者はこれを利用して、ユーザーの操作なしにアカウントを完全に制御できます。



客観的評価

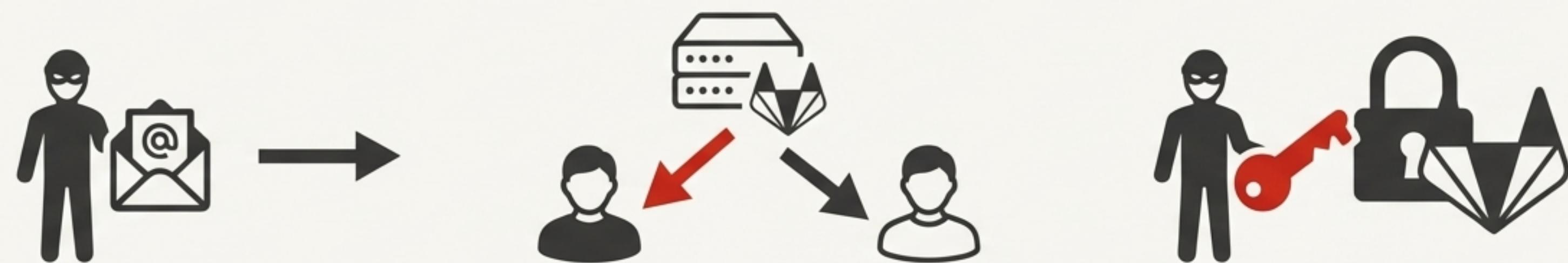
評価指標	スコア/レベル	備考
CVSS 3.1 スコア	9.1 / 10.0 (危機的)	攻撃が容易かつ被害が甚大であることを示す国際標準指標。
GitLab社内評価	Severity 1 (最重要)	GitLabが定める4段階中、最も高い深刻度レベル。
修正SLA	30日以内	GitLabの規定では、発見から30日以内の修正が義務付けられるレベルの緊急性。

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

関連する脆弱性タイプ: CWE-640 (パスワードリセットメカニズムの脆弱性), CWE-284 (不適切なアクセス制御)

脆弱性の仕組みと攻撃シナリオ

攻撃者は、社員のメールアドレスを知っているだけで、被害者の操作なしにアカウントを乗っ取ることが可能です。



1. 攻撃者が特殊な形式で
パスワードリセットを要求。

2. GitLabがリセット用リンクを
正規利用者と攻撃者の両方に
同時送信してしまう。

3. 攻撃者がリンクを悪用し、
アカウントを乗っ取る。

さらに、GitLabの「予測可能なプライベートコミットメール」を悪用すれば、
公開されているメールアドレスを知なくても攻撃が可能となり、リスクを増大させます。

この攻撃は、被害者が不審なメールに気づく前に数分で完了する可能性があり、検知は極めて困難です。

お客様の環境と直面するビジネスリスク

発見された脆弱性は、パスワードリセット機能の致命的な欠陥に起因します。攻撃者はこれを利用して、ユーザーの操作なしにアカウントを完全に制御できます。



お客様のセルフマネージド（SM）環境は、**本脆弱性の影響を受けるバージョン（16.7.2未満）**で稼働しています。
これは、前述の脅威が理論上のリスクではなく、**今そこにある現実の危機**であることを意味します。

想定される最大のリスク

- 知的財産の漏洩：**
 - ソースコード、設計情報、顧客データなど、企業の最重要資産が外部に流出。
- 開発パイプラインの汚染（サプライチェーン攻撃）：**
 - 正規の製品に悪意のあるコード（マルウェア等）が混入され、お客様の顧客やサービス利用者に被害が拡大。
- システムの破壊と事業停止：**
 - CI/CDパイプラインや本番環境のインフラが改ざん・破壊され、サービス提供が不可能になる。

緊急対策の提案 (ACTION REQUIRED)



唯一かつ最善の対策は、システムの一時停止を伴う緊急アップデートの即時実施です。

提案内容:

- 脆弱性が完全に修正された公式バージョン「**16.7.2**」への緊急アップデート。

ダウンタイムが不可避である理由:

- 本修正は、GitLabの基幹部分である「GitLab Rails」へのパッチ適用が必須です。
- 技術的な要請として、適用後、稼働中の全てのサーバー/ノードを再起動する必要があり、システム全体のサービス停止が避けられません。

なぜ「影響調査」を待てないのか？

- 攻撃の痕跡を残しにくいため、侵害の有無を調査する間に攻撃されるリスクが極めて高いです。既知の重大なリスクは、**調査よりも予防 (=アップデート) を最優先することが情報セキュリティの鉄則です。**

求められるご承認事項と今後の流れ

この危機的状況を回避するため、以下の2点について、本日中のご承認をお願い申し上げます。

【ご承認事項】

<input type="checkbox"/>	1. システムの緊急停止	本日夜間帯（具体的な時間帯はご承認後に調整）からのアップデート作業に伴うシステム停止
<input type="checkbox"/>	2. 緊急対応費用の拠出	本アップデート作業に要する費用の予算承認（詳細は別途お見積りを迅速に提示します）

【今後の流れ】

1. ご承認
予定: 本日中
2. 詳細計画のご提示
予定: ご承認後、1時間以内
3. アップデート作業実施
予定: 本日夜間
4. 完了および影響確認報告
予定: 明朝