【緊急】GitLab セキュリティアップデート実施のご提案

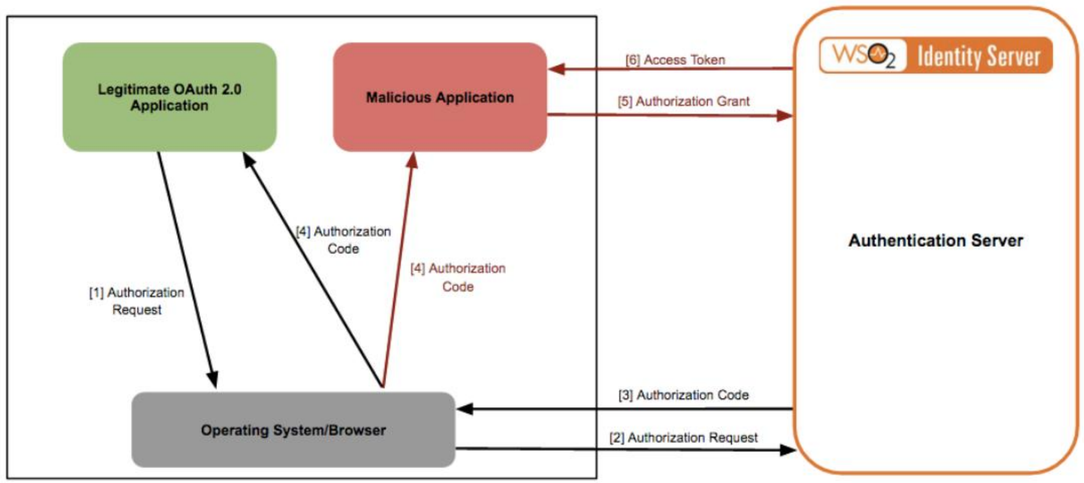
重大な「アカウント乗っ取り」脆弱性への対応と承認依頼

Self-Managed版 環境向け緊急対応資料

脆弱性の実態：パスワードリセット機能の悪用

何が起きているのか

- **通常時:** パスワード再設定メールは「登録された本人のアドレス」のみに送信されます。
- **脆弱性:** システムへの指示を書き換えることで、「被害者」と「攻撃者」の**両方**にメールを送らせることが可能です。
- **結果:** 攻撃者は自分に届いたメールのリンクを使い、被害者のパスワードを強制的に上書きし、乗っ取りを完了させます。



なぜ「緊急対応」が必要なのか

ユーザー操作不要

フィッシング詐欺のようにURLをクリックする必要がありません。社員が休暇中や就寝中であっても、裏で勝手にアカウントが奪われます。(Zero-Click攻撃)

メアドだけで攻撃可能

高度なハッキング技術は不要です。名刺などで公開されている「会社のメールアドレス」さえ知っていれば、誰でも攻撃対象になります。

深刻度 "Critical"

国際的なセキュリティ評価基準（CVSS）において、10点満点中 **9.1** という最高レベルの危険度「Critical」に判定されています。

放置した場合のビジネスリスク

機密情報の流出

開発中のソースコード、設計書、顧客リストなどが外部に持ち出され、競争力の低下や法的責任を問われる恐れがあります。

サプライチェーン攻撃

当社のコードにウイルスを混入され、納品先の顧客システムへ被害を拡大させる「踏み台」にされるリスクがあります。

Self-Managed版のため、我々が手を動かさない限り脆弱性は放置されたままです。

推奨アクションと実施計画

対応策: 修正パッチの適用

既にリリースされている修正版（v16.7.2等）へアップデートを行います。

これにより、メール送信先が「登録ユーザー1名」に厳格に限定され、システムレベルで攻撃を完全に遮断できます。

効果: リスクの完全な排除。

承認のお願い

以下のリソースとスケジュールの承認をお願いします。

- **作業工数:** エンジニア X名 / X人日
- **システム停止:** X時間（夜間・休日実施）
- **実施時期:** 可及的速やかに

Image Sources

https://is.docs.wso2.com/en/6.1.0/assets/img/deploy/authorization-code-grant-type-flow.png

Source: is.docs.wso2.com

https://media.istockphoto.com/id/1349106104/vector/data-breach-concept-internet-security.jpg?s=612x612&w=0&k=20&c=IEnVOwWAyaOJJthCcS36AQj897N68GS6AYBLSQYSF3s=

Source: www.istockphoto.com