GROWI, Inc.

2026.04.23 GROWI SECURITY

GROWI 脆弱性対応のお知らせ (JVN#46728373)

概要

- 弊社が提供している GROWI システムにおいて、未認証ReDos(正規表現によるサービス拒否攻撃)の脆弱性が存在することが判明しました。

該当製品の確認方法

影響を受ける製品は以下の通りです。
製品名称：GROWI
該当バージョン：
・GROWI v7.5.0 およびそれより前のバージョン

脆弱性の説明

- 「GROWI」のUserAgent解析において、**未認証ReDos(正規表現によるサービス拒否攻撃)の脆弱性**が存在します。
- User-Agent解析処理において入力値の長さ制限が行われておらず、細工された長い文字列を送信することでサーバーのCPUリソースを枯渇させることが可能です。

GROWI, Inc.

脆弱性がもたらす脅威

未認証の攻撃者が細工した長いUser-Agentを含むリクエストを送信できる場合、以下の操作が可能です。

- サーバーのCPUリソースを飽和させ、サービス全体を応答不能にする。
- 同時並行でアクセスしている他の利用者のリクエストを大幅に遅延（タイムアウト）させる。

セキュリティ脆弱性の詳細

CVE, JVN が公開している以下のセキュリティアドバイザリ

- JJVN46728373

対策方法

GROWI を v7.5.1 以降のバージョンにアップデートしてください。

アップデート版の入手場所

- GitHub
- Docker Hub

関連ページ

- GROWI.org
- デモサイト
- GROWI Docs
- GitHub

< 一覧へ戻る

GROWI, Inc.

GROWI, Inc.

Tel
03-6233-9447

Mail
info@growi.co.jp

ミッション

お知らせ

採用

ブログ

お問い合わせ