弊社製品 タイム・ワークスにおける脆弱性対応の報告

公開日　2025 年 5 月 30 日
更新日　2025 年 6 月 3 日
京葉システム株式会社

■概要

タイム・ワークス V10 の Web サーバモジュールに脆弱性が存在することが判明しました。
この脆弱性を悪用された場合、悪意ある第三者により、パストラバーサル攻撃が実行されてしまう危険性があります。

CVSS（共通脆弱性評価システム）3.0 にて 脆弱性総合スコア　5.3（警告レベル）
/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/BS:5.3

■該当製品の確認方法

影響を受ける製品は以下の製品です。

製品名称：タイム・ワークス　　対象バージョン：10.0～10.3

■脆弱性の説明及びもたらす脅威

この脆弱性を悪用された場合、悪意ある第三者の攻撃により、同一サーバ上にタイム・ワークス以外の JSON ファイルが存在した場合、読み込まれる可能性があります。

■対策方法

各バージョンに対応した修正パッチを、Web サーバに適用してください。

■関連情報案件名

案件名　　タイム・ワークスにおけるパストラバーサルの脆弱性

取扱番号　　JVN#37075430

■謝辞

GMO サイバーセキュリティ by イエラエ株式会社　安里眞夢様よりこの問題をご報告いただきました。

■連絡先

本件に関するお問い合わせは、こちらまでお願いいたします。

ソフトウェア開発部　脆弱性連絡窓口　psirt@keiyo-system.co.jp