プロダクションプリンター・オフィス向け複合機・スモールオフィス向け複合機の脆弱性対応について

2026年4月23日
キヤノンマーケティングジャパン株式会社

平素はキヤノン製品をご愛用いただき誠にありがとうございます。
プロダクションプリンターとオフィス向け複合機、スモールオフィス向け複合機にて脆弱性が確認されました。
この脆弱性は、ブラウザー経由のリモート管理機能において、管理者権限を取得した第三者が、細工したリクエストにて製品内の宛先表の情報などを取得できる可能性があるというものです。

- CVE-2026-1789

安心して製品をお使いいただくために

本脆弱性を利用した被害は現時点で確認されておりませんが、より安心して製品をお使いいただくため、お持ちの対象製品は、下記対策の実施を推奨致します。

- インターネットに直接接続（グローバルIPアドレスの使用など）せず、ファイアーウォール製品や有線ルーターあるいはWi-Fiルーターで構築した安全なプライベートネットワークからインターネットにアクセスできる環境で、プライベートIPアドレスを設定してご使用ください。
- 初期パスワードが設定されている場合は変更する。
- 管理者と一般ユーザーのID／パスワードが設定できる場合は設定する。
- 各種機能のパスワードなどの設定は、予測しにくい値にする。
- 製品に認証機能がある場合は、その機能を有効にし、製品を利用できるユーザーを管理する。
- 製品に多要素認証機能がある場合は、その機能を有効にし、製品を利用できるユーザーを管理する。
- 製品の設置場所など、物理的なセキュリティに配慮する。

詳細は以下の「製品をネットワークに接続する際のセキュリティ対策について」をご参照ください。

→ 製品をネットワークに接続する際のセキュリティ対策について

上記対策の実施に加えて、一部の製品ではファームウエアアップデートによりセキュリティ機能強化を行っており、これらを適用いただくことでより安全にご使用いただけます。対象製品については下記対象機種一覧PDFをご確認ください。

今後とも引き続き、安心してキヤノン製品をご利用いただきますようお願い申し上げます。

対策が必要なプロダクションプリンター・オフィス向け複合機・スモールオフィス向け複合機

対象機種

- imagePRESSシリーズの一部の機種
- imageFORCEシリーズ
- imageRUNNER ADVANCEシリーズの一部の機種
- imageRUNNERシリーズの一部の機種
- Sateraシリーズの一部の機種

詳細な機種名は「対象機種一覧」をご参照ください。
上記以外の製品の脆弱性については、確認がとれ次第、こちらのページで速やかにご案内致します。

©Canon Marketing Japan Inc.