

Avis technique : Vulnérabilité de sécurité découverte dans les imprimantes CL4/6NX Plus

30 sep 2024

Résumé Certaines imprimantes d'étiquettes SATO présentent des vulnérabilités liées à une autorisation incorrecte/impropre (CWE-863, CWE-287) et à la traversée de répertoires (CWE-22) pouvant affecter leur fonctionnement. Il n'existe aucun cas connu d'exploitation de ces vulnérabilités, et les utilisateurs d'imprimantes ne courent aucun risque de falsification de données ou de divulgation d'informations tant qu'ils prennent des mesures pour protéger leurs systèmes contre les accès non autorisés. Cependant, nous conseillons aux utilisateurs d'appliquer la solution de contournement suivante pour améliorer la sécurité de vos imprimantes.

Imprimantes concernées

- CL4/6NX Plus
- CL4/6NX-J Plus (modèle japonais)

Détails Les imprimantes concernées offrent une fonction WebConfig permettant aux utilisateurs de visualiser ou de modifier les paramètres de l'imprimante via le navigateur web. Cette fonction contient des fonctionnalités nécessitant une connexion utilisateur et peut être vulnérable à une autorisation incorrecte/impropre (CWE-863, CWE-287). Certaines fonctionnalités présentent également une vulnérabilité de traversée de répertoires (CWE-22) permettant aux attaquants de parcourir le système de fichiers et d'accéder à des répertoires restreints. Ces points de vulnérabilité peuvent entraîner des modifications non autorisées des paramètres et la falsification de fichiers, ce qui peut affecter le fonctionnement des imprimantes.

Solution Nous publions une nouvelle mise à jour du firmware de l'imprimante pour corriger les vulnérabilités. Pour obtenir des informations sur la mise à jour du firmware, veuillez contacter votre représentant SATO le plus proche ou le distributeur auprès duquel vous avez acheté le produit.

Contactez-nous afin de [convenir d'un rendez-vous](#).

Solution de contournement Les utilisateurs peuvent contourner les vulnérabilités en activant le pare-feu de l'imprimante et en désactivant la fonction WebConfig. Toutefois, veuillez noter que cette solution est recommandée uniquement si vous ne pouvez pas installer la mise à jour du firmware pour des raisons techniques spécifiques.

Suivez les étapes ci-dessous pour appliquer la solution de contournement. Vous pouvez également vous référer à la section "Paramètres divers du produit" dans notre manuel d'utilisation en ligne pour plus d'informations. (https://www.manual.sato-global.com/printer/cl4nx_cl6nx/main/toc.html)

Activer le pare-feu :

- Allez dans le menu Paramètres de l'imprimante et cliquez sur Interface > Réseau > Avancé > Pare-feu > Activer.

Désactiver WebConfig :

- Allez dans le menu Paramètres de l'imprimante et cliquez sur Interface > Réseau > Avancé > Pare-feu > Autoriser Services et Ports > WebConfig > Désactiver.

Pour toute question ou demande de renseignements, veuillez remplir notre formulaire de contact [ici](#).

当社製ラベルプリンタ製品の脆弱性対応について

2024 年 8 月 30 日

株式会社サトー

概要

当社製ラベルプリンタの一部機種において、複数の脆弱性（不正な認証（CWE-863, CWE-287）、パス・トラバース（CWE-22））が発見されております。本脆弱性により当社製ラベルプリンタの動作に影響を与える可能性があります。

以下に示す対策または、回避策を実施することで、本脆弱性を無効化することが出来ます。

本脆弱性による被害は現時点では確認されておりません。お客様のシステムを経由した不正なアクセスがない限り、データの改ざんや情報漏洩の危険はありませんが、より安心して製品をお使いいただくため、本脆弱性への対応方法等を以下の通りご案内致します。

対象となる製品

当社製品で、本脆弱性に該当し、対策ファームウェアを準備している製品は下記製品となります。

- スキャントロニクス CL4/6NX-J Plus シリーズ
- スキャントロニクス CL4/6NX Plus シリーズ（海外向けモデル）

脆弱性内容

対象製品は、ウェブブラウザから設定確認・設定変更を可能とする WebConfig 機能を搭載しています。この WebConfig 機能の一部機能において認証が不十分（CWE-863, CWE-287）な脆弱性があります。また、WebConfig 機能の一部機能においてデータチェックが不十分（CWE-22）な脆弱性があります。これらの脆弱性により、意図しない設定変更やファイルの改ざんにより、対象製品の動作に影響を与える可能性があります。

対策方法

以下の対策により本脆弱性に対する対策が可能です。

- 対策ファームウェアを適用する。

当社製品の本体ファームウェア更新に関しては、お近くのサトー拠点もしくは商品を購入頂いた販売店へお問い合わせください。作業の依頼は、お問合せください。

回避方法

以下の対策により本脆弱性の回避が可能ですが、当社としましては、前述の対策ファームウェアの適用による対策を推奨します。何らかの理由により対策ファームウェアを適用できない場合は、本回避方法による対策をお願いします。

- ファイアウォール機能を有効にしたうえで、WebConfig 機能を無効とする。本対策では、対策ファームウェアの適用は不要です。ファイアウォール機能の有効化および、WebConfig 機能の無効化は、以下のオンラインマニュアルの記載を参照願います。
 - オンラインマニュアル：<https://www.sato.co.jp/webmanual/printer/clnx-jplus/main/toc.html>
 - ✧ ファイアウォール設定： 本製品の [設定] メニュー > [通信設定] メニュー > [ネットワーク] > [詳細設定] > [ファイアウォール] > [有効]
 - ✧ WebConfig 設定： 本製品の [設定] メニュー > [通信設定] メニュー > [ネットワーク] > [詳細設定] > [ファイアウォール] > [許可するサービス・ポート] > [WebConfig] > [無効]

本件に関するお問い合わせ先

本件に関するお問い合わせは、お客様ヘルプデスクにて承ります。

電話による問い合わせ： 0120-696310（受付時間：24 時間 365 日）

お問い合わせフォーム：<https://www.sato.co.jp/contact/support/>

