Doradztwo techniczne: Wykryta luka w zabezpieczeniach drukarek CL4/6NX Plus

30 sierpnia 2024

Podsumowanie

W niektórych drukarkach etykiet SATO wykryto luki w zabezpieczeniach dotyczące nieprawidłowej/nieodpowiedniej autoryzacji (CWE-863, CWE-287) oraz przejścia ścieżki (CWE-22), co może prowadzić do nieautoryzowanych zmian ustawień i manipulacji plikami, a w rezultacie wpływać na działanie drukarek

Nie są znane przypadki wykorzystania tych luk, a użytkownicy drukarek nie są narażeni na manipulacje danymi ani ujawnienie informacji, pod warunkiem, że podejmują środki ochrony swoich systemów przed nieautoryzowanym dostępem. Niemniej jednak zalecamy użytkownikom zastosowanie następującego rozwiązania dla drukarek w celu poprawy bezpieczeństwa.

Modele objęte problemem

- CL4/6NX Plus
- CL4/6NX-J Plus (Japan model)

Rozwiązanie

Wydajemy nową aktualizację oprogramowania sprzętowego drukarki w celu załataniu luk w zabezpieczeniach. Aby uzyskać informacje na temat aktualizacji oprogramowania, prosimy o kontakt z najbliższym przedstawicielem SATO lub dystrybutorem, u którego zakupiono drukarkę. **Prosimy o kontakt w celu umówienia się na spotkanie.**

Obejście

Użytkownicy mogą obejść luki w zabezpieczeniach, włączając zaporę sieciową drukarki i wyłączając funkcję WebConfig, gdy instalacja aktualizacji oprogramowania sprzętowego jest niemożliwa z powodu określonych przyczyn technicznych. Należy pamiętać, że obejście jest tymczasowe i w idealnym przypadku należy usunąć luki w zabezpieczeniach poprzez instalację łatki bezpieczeństwa, gdy tylko sytuacja na to pozwoli.

- Postępuj zgodnie z poniższymi krokami, aby zastosować rozwiązanie obejściowe. Możesz również zapoznać się z sekcją „Różne ustawienia produktu" w naszym internetowym podręczniku użytkownika, aby uzyskać więcej informacji. (https://www.manual.sato-global.com/printer/cl4nx_cl6nx/main/toc.html)

    - Włącz zaporę sieciową: Przejdź do menu Ustawienia drukarki i kliknij Interfejs > Sieć > Zaawansowane > Zaporę sieciowa > Włącz.
    - Wyłącz WebConfig (funkcja przeglądania lub zmiany ustawień drukarki za pomocą przeglądarki internetowej): Przejdź do menu Ustawienia drukarki i kliknij Interfejs > Sieć > Zaawansowane > Zaporę sieciową > Zezwól na usługi i porty > WebConfig > Wyłącz.

W przypadku pytań i zapytań prosimy o wypełnienie naszego formularza kontaktowego tutaj.

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・トラバーサル（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、お客様ヘルプディスクにて承ります。

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/