Technical advisory: Security vulnerability discovered in CL4/6NX Plus printers

September 30, 2024

Summary

Some SATO label printers were found to have vulnerabilities regarding incorrect/improper authorization (CWE-863, CWE-287) and path traversal (CWE-22) that may lead to unauthorized setting changes and file tampering, potentially impacting how printers operate.

There are no known cases of these vulnerabilities being exploited, and printer users are not at risk of data tampering or information exposure as long as users take measures to protect their systems from unauthorized access.

However, we advise users to apply the following solution to your printers for improved security.

Affected printers

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

Solution

We are releasing a new printer firmware update to patch the vulnerabilities. For information on updating the firmware, please contact your nearest SATO representative or the distributor where you purchased the printer. **Please contact us to arrange for an appointment.**

Work-around

Users can work around the vulnerabilities by enabling the printer's firewall and disabling the WebConfig function, if you cannot have the firmware update installed due to certain technical reasons. Please note that the work-around is temporary, and that you should ideally remediate the vulnerabilities through the security patch once your situation allows for it.

- Follow the steps below to apply the work-around. You can also refer to the "Various Settings of the Product" section in our online user manual for more information. (https://www.manual.sato-global.com/printer/cl4nx_cl6nx/main/toc.html)
  - Enable firewall:
    Go to the printer's Settings menu and click Interface> Network> Advanced> Firewall> Enable.
  - Disable WebConfig (function for viewing or changing printer settings via web browser):
    Go to the printer's Settings menu and click Interface> Network> Advanced> Firewall> Allow Services and Ports> WebConfig> Disable.

For questions and inquiries, please fill out our contact form here.

<新>

当社製ラベルプリンタ商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

平素より、当社製品をご愛顧いただき誠にありがとうございます。
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）、データチェック（CWE-22）を確認しています。本脆弱性により、お客さまのシステム環境内で意図しない設定変更やファイルの改ざんなど、対象商品の動作に影響を与える可能性があります。
お客さま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なく、現時点で本脆弱性による被害は確認されておりません。
より安心して当社商品をお使いいただくため、本脆弱性を無効化する対策方法等を以下の通りご案内いたします。

対象商品

- 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）

対策方法

以下の対策により本脆弱性を無効化することが可能です。

- 対策ファームウェアを適用する。

当社商品の本体ファームウェア更新後に、各種機能設定、ご使用のサプライに対する印字位置などの各種設定が必要になることがあります。そのため、ファームウェアの更新作業に関しては、当社 CE が作業いたします。作業の依頼は、下記問い合わせ先、または担当 CE へお問い合わせください。

回避方法

現在、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、以下の対策により本脆弱性の回避が可能です。なお、本回避方法による対策後も、当社としましては前述の対策ファームウェアの適用を推奨しますので、対策ファームウェアの適用が可能になりましたら、下記お問い合わせ先、または担当 CE へご連絡ください。

- 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（お客様ヘルプデスク）

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/