Aviso técnico: Vulnerabilidad de seguridad descubierta en impresoras CL4/6NX Plus

30 de septiembre de 2024

Resumen

Se descubrió que algunas impresoras de etiquetas SATO tenían vulnerabilidades relacionadas con la autorización incorrecta (CWE-863, CWE-287) y el recorrido de ruta (CWE-22) que pueden provocar cambios de configuración no autorizados y manipulación de archivos, lo que podría afectar el funcionamiento de las impresoras.

No se conocen casos de explotación de estas vulnerabilidades, y los usuarios de impresoras no corren el riesgo de sufrir la manipulación de datos o la exposición de la información, siempre que los usuarios tomen medidas para proteger sus sistemas del acceso no autorizado.

Sin embargo, aconsejamos a los usuarios que apliquen la siguiente solución a sus impresoras para mejorar la seguridad.

Impresoras afectadas

- CL4/6NX Plus
- CL4/6NX-J Plus (modelo Japón)

Solución

Estamos lanzando una nueva actualización de firmware de la impresora para parchear las vulnerabilidades. Para obtener información sobre cómo actualizar el firmware, póngase en contacto con el representante de SATO más cercano o con el distribuidor donde adquirió la impresora.

Póngase [en contacto con nosotros](#) para concertar una cita.

Solución alternativa

Los usuarios pueden solucionar las vulnerabilidades habilitando el firewall de la impresora y desactivando la función WebConfig,. Si no puede tener instalada la actualización de firmware debido a ciertas razones técnicas. Tenga en cuenta que la solución alternativa es temporal y que lo ideal es remediar las vulnerabilidades a través del parche de seguridad una vez que su situación lo permita.

- Siga los pasos que se indican a continuación para aplicar la solución alternativa. También puede consultar la sección "Varias configuraciones del producto" en nuestro manual de usuario en línea para obtener más información. (https://www.manual.sato-global.com/printer/cl4nx_cl6nx/main/toc.html)
 - Habilitar firewall:
Vaya al menú Configuración de la impresora y haga clic en Interfaz> Red> Avanzado> Firewall> Habilitar.
 - Deshabilitar WebConfig (función para ver o cambiar la configuración de la impresora a través del navegador web):
Vaya al menú Configuración de la impresora y haga clic en Interfaz> Red> Avanzado> Firewall> Permitir servicios y puertos> WebConfig> Deshabilitar.

Para preguntas y consultas, rellene nuestro formulario de contacto [aquí](#).

<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、お客様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/>