

## **Avis complémentaire concernant la vulnérabilité de sécurité découverte dans les imprimantes CL4/6NX Plus**

04/08/2025  
SATO Europe

### **Résumé**

En plus des vulnérabilités déjà identifiées (CWE-22, CWE-287 et CWE-863), deux nouvelles vulnérabilités — CWE-78 et CWE-434 — ont été confirmées.

Des contre-mesures appropriées pour ces nouveaux problèmes ont déjà été mises en œuvre.

Pour plus de détails, veuillez vous référer aux sections ci-dessous intitulées [Solution] ou [Mesure de contournement].

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

---

## **Vulnérabilité de sécurité découverte dans les imprimantes CL4/6NX Plus**

04/08/2025  
SATO Europe

### **Résumé**

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.

### **Imprimantes concernées**

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

### **Solution**

Nous publions une nouvelle mise à jour du micrologiciel des imprimantes afin de corriger les vulnérabilités. Pour obtenir des informations sur la mise à jour du micrologiciel, veuillez contacter votre représentant SATO le plus proche ou le distributeur auprès duquel vous avez acheté l'imprimante. Merci de nous contacter pour fixer un rendez-vous [contact us](#)

## Mesure de contournement

Si vous ne pouvez pas installer la mise à jour du micrologiciel pour des raisons techniques, vous pouvez limiter les risques en activant le pare-feu de l'imprimante et en désactivant la fonction WebConfig.

Veuillez noter que cette mesure de contournement est temporaire, et que vous devriez idéalement corriger les vulnérabilités par le biais du correctif de sécurité dès que possible.

Procédure pour appliquer la mesure de contournement (vous pouvez aussi consulter la section [Divers réglages du produit](#) de notre manuel d'utilisation en ligne pour plus d'informations) :

### Activer le pare-feu

Accédez au menu Settings de l'imprimante, puis cliquez sur :

Interface > Network > Advanced > Firewall > Enable.

### Désactiver WebConfig

(fonction permettant de visualiser ou modifier les paramètres de l'imprimante via un navigateur web)

Accédez au menu Settings de l'imprimante, puis cliquez sur :

Interface > Network > Advanced > Firewall > Allow Services and Ports > WebConfig > Disable.

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