關於 CL4/6NX Plus 印表機中發現的安全漏洞補充通知

2025 年 8 月 4 日

摘要

除了先前發現的漏洞（CWE-22、CWE-287 和 CWE-863）之外，我們還確認了兩個新漏洞：CWE-78 和 CWE-434。我們已針對這些新發現的問題採取了相應的措施。更多詳情，請參閱下方標題為[解決方案]或[臨時措施]的部分。如有任何問題或疑問，請在此填寫我們的聯絡表單。

CL4/6NX Plus 印表機發現安全漏洞

2024 年 9 月 30 日

摘要

部分 SATO 標籤印表機被發現存在與不正確/不當授權（CWE-863、CWE-287）和路徑（CWE-22）相關的漏洞，這些漏洞可能導致未經授權的設定變更和文件篡改，從而可能影響印表機的運作。目前尚無此類漏洞被利用的已知案例，只要印表機使用者採取措施保護其系統免受未經授權的訪問，就不會面臨資料篡改或資訊外洩的風險。但是，我們仍建議使用者對印表機套用以下解決方案，以提高安全性。

受影響的印表機型號

- CL4/6NX Plus
- CL4/6NX-J Plus (日本機種)

解決方案

我們正在發布新的印表機韌體更新來修補這些漏洞。有關韌體更新的訊息，請聯繫您附近的 SATO 代表或您購買印表機的經銷商。請聯絡我們預約。

解決方法

如果由於某些技術原因無法安裝韌體更新，用戶可以透過啟用印表機防火牆並停用 WebConfig 功能來規避這些漏洞。請注意，此解決方法是暫時的，理想情況下，您應該在情況允許時透過安全修補程式修復這些漏洞。

・請依照以下步驟操作以套用此解決方法。您也可以參考我們線上使用手冊中的「產品各項設定」部分以了解更多資訊。

啟用防火牆

進入印表機的「設定」選單，點選「介面」>「網路」>「進階」>「防火牆」>「啟用」。

停用 WebConfig（透過 Web 瀏覽器檢視或變更印表機設定的功能）

進入印表機的「設定」選單，點選「介面」>「網路」>「進階」>「防火牆」>「允許服務和連接埠」>「WebConfig」>「停用」。

如有任何問題或疑問，請在此填寫我們的聯絡表單。