

印表機與掃描器 Epson Web Config 設定功能之安全性漏洞通知

Issued on: July 7, 2026

Seiko Epson Corporation

Epson Sales Japan Corporation

感謝您對 Epson 產品的支持與愛護。

我們在此通知您，經確認部分印表機及掃描器產品的 Epson Web Config 設定功能存在安全性漏洞。Epson Web Config 為一項可透過網頁瀏覽器存取的管理功能，使用者可藉此檢視裝置狀態及變更各項設定。

為降低潛在風險並確保產品使用安全，建議您檢查相關產品是否受到影響，並依照 Epson 提供的指引執行必要的更新措施。

■ 已知漏洞

這是一個跨站請求偽造（CSRF）漏洞。

如果使用者造訪第三方建立的惡意網站，受影響裝置設定有可能透過 Epson Web Config 設定介面被竄改。

■ 漏洞影響

目前尚未確認有利用此漏洞的事件發生。

■ 受影響機型

L5590 / L3560 / L3556 / L3550 / L8050 / L18050 / L11050 / M2050 / XP-2200 / WF-2930 /
XP-4101 / XP-2101 / WF-2831 / M2120 / M2110 / L14150 / L6290 / L6270 / L4260 / L5290 /
L3260 / L3250 / L3256 / L6490 / L3150 / L3156 / L5190 / L5196 / M1120 / M3170 / M2170 /
M1170 / L4150 / L4160 / L6170 / L6190 / XP-15010 / WF-2861 / WF-100 / SC-F130 /

（註）以上未列出的產品不受此漏洞影響。

■ 解決方法

為確保您的產品安全可靠地使用，請參閱以下網址的安全指南：URL: [Security for printers and MFPs](#)

<基於安全指南的安裝與設定（第3章）>

1. 請勿將產品直接連接到網際網路，建議將產品安裝於防火牆保護網路環境中，並使用私人 IP 位址進行存取與管理。

<與此問題相關的操作注意事項>

2. 使用管理員帳號登入 Web 設定頁面完成必要操作後，請務必立即登出，避免長時間維持管理員登入狀態。

3. 使用管理員帳號登入期間，請勿瀏覽不明或可疑網站、點擊來源不明的連結、開啟未知檔案，或進行其他可能造成安全風險的操作。

■ 愛普生安全措施

有關安全指南的更多信息，請參閱愛普生產品連接到網路時的注意事項：[Precautions When Connecting Epson Products to a Network](#)