

## 기술 자문: CL4/6NX Plus 프린터에서 발견된 보안 취약성

2024 년 9 월 30 일

### 요약

일부 SATO 라벨 프린터는 잘못된/부적절한 권한 부여(CWE-863, CWE-287) 및 경로 횡단(CWE-22)에 대한 취약성이 발견되어 무단 설정 변경 및 파일 변조를 초래하여 프린터 작동 방식에 영향을 미칠 수 있습니다.

이러한 취약점이 악용되는 사례는 알려진 바가 없으며, 사용자가 시스템을 무단 액세스로부터 보호하기 위한 조치를 취하는 한 프린터 사용자는 데이터 조작이나 정보 노출의 위험이 없습니다. 그러나 보안을 강화하기 위해 사용자에게 다음 솔루션을 프린터에 적용할 것을 권장합니다.

### 적용되는 프린터

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

### 솔루션

취약점을 패치하기 위해 새로운 프린터 펌웨어 업데이트를 출시합니다. 펌웨어 업데이트에 대한 자세한 내용은 가까운 SATO 담당자 또는 프린터를 구입한 유통업체에 문의하십시오.

### 해결방법

사용자는 프린터의 방화벽을 활성화하고 WebConfig 기능을 비활성화함으로써 취약성을 해결할 수 있습니다. 특정 기술적 이유로 펌웨어 업데이트를 설치할 수 없는 경우 이를 해결하기 위한 일시적인 것이며, 상황이 허락하면 보안 패치를 통해 취약성을 이상적으로 업데이트해야 합니다.

λ 아래 단계에 따라 해결 방법을 적용하십시오. 자세한 내용은 온라인 사용 설명서의 "제품의 다양한 설정" 섹션을 참조하십시오.

([https://www.manual.sato-global.com/printer/cl4nx\\_cl6nx/main/toc.html](https://www.manual.sato-global.com/printer/cl4nx_cl6nx/main/toc.html))

→ 방화벽 사용:

프린터의 Settings(설정) 메뉴로 이동하여 Interface(인터페이스) > Network(네트워크) > Advanced(고급) > Firewall(방화벽) > Enable(활성화)을 클릭합니다.

→ WebConfig 사용 안 함(웹 브라우저를 통해 프린터 설정을 보거나 변경하기 위한 기능):  
프린터의 설정 메뉴로 이동하여 인터페이스 > 네트워크 > 고급 > 방화벽 > 서비스 및 포트 허용 > WebConfig > 사용 안 함을 클릭합니다.

질문 및 요청 사항은 [여기](#)에 저희 연락처 양식을 작성해 주시기 바랍니다.