

## CL4/6NX Plus 프린터에서 발견된 보안 취약점에 관한 추가 공지 사항

2025 년 9 월 1 일

### 요약

이러한 취약점에 대한 문의를 받았으므로 추가 정보를 제공하고자 합니다.

### 영향을 받는 프린터

- CL4NX Plus(1.15.5-r1 이전 버전의 펌웨어)
- CL6NX Plus(1.15.5-r1 이전 버전의 펌웨어)
- CL4NX-J Plus(일본 모델)(1.15.5-r1 이전 펌웨어 버전)
- CL6NX-J Plus(일본 모델)(1.15.5-r1 이전 펌웨어 버전)

### 프린터의 펌웨어 버전을 확인하는 방법

펌웨어 버전을 확인하는 방법은 온라인 "[작업 설명서](#)"를 참조하시기 바랍니다.  
TOP > 제품의 다양한 설정 > 제품의 [설정] 메뉴 > [정보] 메뉴 > [구축 버전]

### 해결방안

다음 조치 중 하나를 구현하여 이 취약점을 비활성화할 수 있습니다.

### 프린터 설정 변경

---

#### 프린터 설정 변경 방법

방화벽 기능을 활성화하고 WebConfig 페이지에 대한 액세스를 비활성화합니다.  
프린터 설정을 변경하는 방법은 온라인 "[운영자 설명서](#)"를 참조하시기 바랍니다.

#### 방화벽

TOP > 제품의 다양한 설정 > 제품의 [설정] 메뉴 > [인터페이스] 메뉴 > [네트워크] > [고급] > [방화벽]

## WebConfig

TOP > 제품의 다양한 설정 > 제품의 [설정] 메뉴 > [인터페이스] 메뉴 > [네트워크] > [고급] > [방화벽] > [서비스 및 포트 허용]

### 웹 브라우저를 사용하여 설정을 변경하는 고객

더 이상 웹 브라우저를 통해 프린터 설정을 변경할 수 없기 때문에, 프린터 설정을 변경하려면 다음 방법 중 하나를 사용하세요:

- 프린터의 LCD 패널에서 설정 변경
- "올인원 툴" 애플리케이션 사용

### 펌웨어 업데이트 설치

---

취약점을 보완하기 위해 새로운 프린터 펌웨어 업데이트를 출시합니다. 펌웨어 업데이트에 대한 자세한 내용은 가까운 SATO 담당자 또는 프린터를 구매한 유통업체에 문의하시기 바랍니다. 예약을 원하시면 저희에게 연락해 주세요.

질문과 문의 사항이 있으시면, [여기에](#) 저희 연락처 양식을 작성해 주시기 바랍니다.

---

## CL4/6NX Plus 프린터에서 발견된 보안 취약점에 관한 추가 공지 사항

2025 년 8 월 4 일

### 요약

이전에 확인된 취약점(CWE-22, CWE-287, CWE-863) 외에도 두 가지 새로운 취약점인 CWE-78 과 CWE-434 가 확인되었습니다.

새로 확인된 문제들에 대한 적절한 대응책이 이미 시행되었습니다.

자세한 내용은 아래의 [대책] 또는 [해결 방법] 섹션을 참조하시기 바랍니다.

질문과 문의 사항이 있으시면, [여기에](#) 저희 연락처 양식을 작성해 주시기 바랍니다.

---

# CL4/6NX Plus 프린터에서 발견된 보안 취약점

2024 년 9 월 30 일

## 요약

일부 SATO 라벨 프린터는 잘못된/부적절한 권한 부여(CWE-863, CWE-287)와 경로 탐색(CWE-22)에 대한 취약점이 발견되어 무단 설정 변경 및 파일 변조가 발생할 수 있으며, 이는 프린터 작동 방식에 영향을 미칠 수 있습니다.

이러한 취약점이 악용된 사례는 아직 알려진 바 없으며, 사용자가 무단 액세스로부터 시스템을 보호하기 위한 조치를 취하는 한 프린터 사용자는 데이터 변조나 정보 노출의 위험에 처하지 않습니다. 그러나 보안을 개선하기 위해 다음 솔루션을 프린터에 적용할 것을 권장합니다.

## 영향을 받는 프린터

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

## 해결방안

취약점을 보완하기 위해 새로운 프린터 펌웨어 업데이트를 출시합니다. 펌웨어 업데이트에 대한 자세한 내용은 가까운 SATO 담당자 또는 프린터를 구매한 유통업체에 문의하시기 바랍니다. 예약을 원하시면 저희에게 연락해 주세요.

## 해결방법

사용자는 특정 기술적 이유로 펌웨어 업데이트를 설치할 수 없는 경우 프린터의 방화벽을 활성화하고 WebConfig 기능을 비활성화하여 취약점을 해결할 수 있습니다. 이 해결 방법은 일시적이며 상황이 허락하면 보안 패치를 통해 취약점을 수정하는 것이 이상적입니다.

.아래 단계를 따라 해결 방법을 적용하세요. 자세한 내용은 온라인 사용 설명서의 "[제품의 다양한 설정](#)" 섹션을 참조할 수도 있습니다

## 방화벽 사용

프린터의 설정 메뉴로 이동하여 인터페이스 > 네트워크 > 고급 > 방화벽 > 활성화를 클릭합니다.

## WebConfig 비활성화(웹 브라우저를 통해 프린터 설정을 보거나 변경하는 기능)

프린터의 설정 메뉴로 이동하여 인터페이스 > 네트워크 > 고급>을 클릭합니다  
방화벽> 서비스 및 포트 허용> 웹구성> 비활성화.

질문과 문의 사항이 있으시면, [여기에](#) 저희 연락처 양식을 작성해 주시기 바랍니다.