

[공식 성명] 펌웨어 복화화키 노출

2025.06.13

한화비전 사이버보안팀 (S-CERT)

한화비전은 최근 특정 한화비전 카메라 제품에 대한 보안 분석 내용이 담긴 블로그 게시물 및 유튜브 영상의 존재를 인지하게 되었습니다. 한화비전 사이버보안팀(S-CERT)의 조사 및 검토 결과, 문제 상황은 다음의 카메라 제품에만 해당됨을 확인했습니다.

- Wisenet5 기반 X/T 시리즈, Wisenet Q시리즈, Wisenet A시리즈, 그리고, 구 PNM 멀티센서 카메라

현재까지 이 카메라 제품과 관련된 보안 침해나 심각한 데이터 유출 사례는 보고되지 않았음을 고객 여러분께 알려드립니다. 영상 및 블로그 내용에 대한 분석과 관련 리스크, 그리고 완화 방안에 대한 요약 내용은 아래와 같습니다:

■ 게시된 블로그/영상 내용의 요약

- “Chip-off + 플래시 메모리 덤프” 기술을 이용한 카메라 펌웨어 분석. 분석은 네트워크 상의 장치를 통하지 않고 수행되었습니다.
- 펌웨어내 암호화키가 노출

■ 리스크 평가

- 해당 영상에서 확인된 특정 구형 카메라 모델에 대하여 악의적인 의도로 펌웨어를 수정할 가능성이 있습니다. 단, 모든 한화비전 네트워크 기기들은 **비밀번호 기반 접근제어로 보호되며, 인증 정보 없이는 수정된 펌웨어를 기기에 설치할 수 없습니다.**
- 본 문제는 시큐어 업데이트 또는 시큐어 부트가 지원되지 않는 다수의 기존 IoT 장비들에게는 동일한 영향이 있는 리스크입니다.

■ 리스크 완화 방안

- 한화비전 공식 홈페이지¹ 또는 한화비전에서 제공된 Wisenet 디바이스 매니저를 통해 배포되는 **펌웨어만 사용** 권장
- 비인가 펌웨어 설치를 예방하기 위해 최신 펌웨어 적용
- 모든 카메라의 관리자 비밀번호에 대해 강력한 비밀번호로 관리

¹ 한화비전의 공식 홈페이지는 다음과 같습니다:

- <https://www.hanwhavision.com>
- <https://www.hanwhavisionamerica.com>
- <https://www.hanwhavisionsupport.com>
- <https://www.hanwhavision.eu>

■ 보안 강화 방안

- 영향을 받는 레거시 카메라 모델에 대해 노출된 암호화키를 업데이트하고 펌웨어 전자서명 검증을 구현하여 카메라가 승인되지 않은 펌웨어 파일을 거부하도록 함
※ 최신 모델들은 이미 펌웨어 전자서명 검증 기능이 적용되어 있어 본 문제의 영향이 없습니다.

당사는 모든 제품의 보안 문제점을 해결하고 고객의 신뢰를 지키기 위해 최선을 다하고 있습니다. 펌웨어 패치 및 추가 업데이트는 한화비전의 공식 홈페이지를 통해서만 배포됩니다. 모든 사용자께서는 반드시 한화비전 공식 홈페이지에서만 제공되는 최신 펌웨어를 다운로드하여 설치하시기를 강력히 권장합니다.