KISA 한국인터넷진흥원	보도자료	대체불가 대한민국
2026. 11. 13.(금) 조간[온라인: 11. 12.(목) 12:00]부터 보도 가능합니다.		

담당부서	디지털AI제품인증팀 최윤선 팀장(전화: 02-405-5130, 전자우편: yschoi@kisa.or.kr) 디지털AI제품인증팀 최진우 선임(전화: 02-405-5133, 전자우편: indra4812@kisa.or.kr)	
참고자료	사진 있음 ■ 사진 없음 □	총 3매

시중 유통 아이피(IP) 카메라 10개 제품 보안 점검

한국인터넷진흥원(KISA)은 한국소비자원(원장 윤수현)과 함께 시중에 유통 중인 아이피(IP) 카메라 10개 제품*의 보안성을 점검하고, 사생활 침해 가능성 등 보안 취약점이 발견된 제품 제조사에 신속한 개선을 권고했다고 2026. 11. 12.(목) 밝혔다.

* 다후아 DH-H3B, 로보뷰 GI-ROBOA7(RoboView A7), 브이스타캠 VSTARCAM-800X, 샤오미 MJSXJ16CM(C500 PRO), 아이피타임 C500G, 이글루 TSC-443P(S8), 타포 TC74, 파인뷰 K11, 하이크비전 CN-D1153G, 헤이홈 GKW-MC0511(스마트 홈카메라 Pro+) (총 10개, 가나다순)

아이피(IP) 카메라는 네트워크에 연결돼 원격으로 영상을 실시간 확인할 수 있는 사물인터넷(IoT) 제품이다. 방범·모니터링 목적으로 가정과 소형 사무실에서 널리 사용되고 있으나, 보안이 미흡할 경우 영상 유출 등 사생활이 침해될 수 있어 이용에 각별한 주의가 필요하다.

이에 한국인터넷진흥원과 한국소비자원은 온라인 쇼핑몰 판매 순위, 소비자 설문조사 결과 등을 고려해 아이피(IP) 카메라 10개 제품을 선정하고 보안성을 점검했다.

점검은 ▲하드웨어, 네트워크, 펌웨어 등 '기기 분야' ▲아이피(IP) 카메라 제어·설정을 담당하는 '모바일 앱 분야' ▲제조사 보안 업데이트 정책, 개인정보 보호정책 등 '정책·관리 분야'로 나눠 총 37개 항목으로 진행됐다.

시험대상 아이피(IP) 카메라 10개 제품을 대상으로 보안 전문인력의 고도화된 공격 시나리오에 기반해 보안 취약점을 점검*한 결과, 전반적으로 개선이 필요했고 3개 제품은 사용자 인증 절차가 미비했다.

* 기기(하드웨어, 네트워크, 펌웨어) 분야, 모바일 앱 분야, 정책·관리 분야 취약점 등 총 37개 항목 점검 수행 결과 등 취약점 특이 사항을 종합해 평가

사용자 인증 절차가 미비한 3개 제품*에서는 공격자가 타인의 아이피(IP) 카메라가 촬영한 이미지, 영상 등을 무단으로 내려받거나, 카메라 기능을 강제로 활성화하거나 조작할 수 있는 등 사생활이 노출될 수 있는 보안 취약점이 확인됐다.

* 로보뷰 GI-ROBOA7(RoboView A7), 브이스타캠 VSTARCAM-800X, 파인뷰 K11

점검 영역(기기 분야, 모바일 앱 분야, 정책·관리 분야)별 대표 취약점은 다음과 같다.

기기 분야에서는 ▲4개 제품*에서 노출된 테스트 단자가 활성화돼 있어 시스템 접근·정보 유출 위험이 존재하는 경우 ▲8개 제품**에서 안전한 통신 프로토콜을 사용하지 않아 통신 구간에서 사용자 데이터 유출이 가능한 경우 ▲모든 제품에서 펌웨어 보안 설정이 미흡한 경우 등의 취약점이 확인됐다.

* 브이스타캠 VSTARCAM-800X, 이글루 TSC-443P(S8), 파인뷰 K11,
헤이홈 GKW-MC0511(스마트 홈카메라 Pro+)

** 다후아 DH-H3B, 로보뷰 GI-ROBOA7(RoboView A7), 브이스타캠 VSTARCAM-800X, 아이피타임 C500G, 이글루 TSC-443P(S8), 타포 TC74, 파인뷰 K11, 하이크비전 CN-D1153G

모바일 앱 분야에서는 5개 제품*에서 안전한 패스워드 정책**이 적용되지 않아 개선이 필요했다.

* 다후아 DH-H3B, 브이스타캠 VSTARCAM-800X, 샤오미 MJSXJ16CM(C500 PRO), 아이피타임 C500G, 타포 TC74

** 대소문자, 숫자, 특수문자 중 3개 조합 8자리 이상 또는 2개 조합 10자리 이상 패스워드 설정 등

정책·관리 분야 점검에서는 보안 업데이트 지원 기간 확인이 불가능한 6개 제품*이 발견됐다.

* 로보뷰 GI-ROBOA7(RoboView A7), 브이스타캠 VSTARCAM-800X, 아이피타임 C500G, 이글루 TSC-443P(S8), 파인뷰 K11, 헤이홈 GKW-MC0511(스마트 홈카메라 Pro+)

한국인터넷진흥원은 사생활 유출 우려가 있는 취약점이 확인된 3개 제품 제조사에 신속한 개선을 권고했다. 현재 2개 제품(로보뷰, 파인뷰)은 조치가 완료됐으며, 1개 제품은 조치가 진행 중이다.

이와 함께 한국인터넷진흥원은 점검 대상이 된 10개 제품 제조사에 점검 결과와 조치 방법 등을 공유했다. 이들 기업은 점검 결과에 따라 한국소비자원에 품질개선 계획을 제출했으며, 한국인터넷진흥원은 제출된 계획의 이행 여부를 지속 점검할 예정이다.

한편, 이번 점검은 2025년 로봇청소기 안전 실태 조사에 이어 생활 밀착형 디지털제품을 대상으로 벌인 두 번째 공동 보안 점검이다. 한국인터넷진흥원과 한국소비자원은 국민 생활과 밀접한 디지털제품의 보안성을 높이고 소비자를 보호하기 위한 협력을 이어갈 계획이다.

한국인터넷진흥원 이용필 디지털위협예방본부장은 “안전한 디지털제품 사용을 위해 제조·유통사에서는 개발부터 폐기까지 전주기에 보안을 적용해 안전하고 책임 있는 유통 체계를 구축하고, 소비자는 생활 속 보안 습관을 실천해 주시길 바란다”며 “앞으로도 관계 기관과 협력해 생활 밀착형 디지털제품의 보안 취약점을 선제적으로 발굴·개선하며 국민이 안심할 수 있는 디지털 이용 환경을 조성해 나가겠다”고 말했다.

붙임 1 'IP카메라 품질비교시험(보안 취약점 점검)' 개요

1 점검 목적

□ 지속적으로 디지털제품(가정용 IP카메라) 해킹 등 영상 유출로 인한 피해가 발생하고 있어, 「IP카메라 보안 관리체계 고도화 방안('25.12.7, 과기정통부)」 후속대책 및 국내 소비자의 안전 확보를 위해 「소비자기본법」 제35조 및 제51조에 근거하여 보안 취약점 점검을 진행함.

2 점검 대상

□ 시중에 판매·유통 중인 IP카메라 10종

※ 조사대상은 국내 시장 기준 판매량이 높은 브랜드 및 소비자 설문조사 등을 중심으로 선정함.

3 점검 내용 및 방법

□ IP카메라 대상 보안 취약점 등 보안성 점검

<점검내용 및 방법>

내용			방법
• 국내외 보안 표준 및 기준 검토			문헌 조사
• 보안 점검			보안성 점검
① 기기	하드웨어	USB 및 디버깅 포트 등 IP카메라의 내·외부 물리적 인터페이스	
	네트워크	IP카메라와 모바일 앱, 서버 간 통신을 위한 연결 수단	
	펌웨어	IP카메라 내부의 시스템 제어 및 동작 로직 소프트웨어	
②모바일 앱		사용자가 IP카메라를 제어하고 설정할 수 있는 스마트폰 기반 애플리케이션	
③정책 관리		제조사의 취약점 공개 정책, 보안 업데이트 정책, 개인정보 보호정책	

※ 보안 전문 인력의 고도화된 공격 시나리오를 기반으로 점검

※ (국내) IoT 보안인증(KISA), 국정원 보안요구사항, (국외) EN 303 645(ETSI)*, OWASP**(ISTG (IoT보안), MAS(모바일보안)) 등 참고하여 총 **37개 항목**(**기기**(하드웨어·네트워크·펌웨어) **19개, 모바일 앱 15개**, **정책 관리 3개)**

* (EN 303 645) 유럽전기통신표준협회(ETSI)에서 제정한 소비자용 IoT 제품의 보안 요구사항 표준

** (OWASP, Open Worldwide Application Security Project) 오픈 웹 애플리케이션 보안 프로젝트로 웹·모바일·IoT 등 분야별 보안 취약점과 대응 방안을 정리한 국제 오픈 보안 가이드

4 점검 기간

□ 2026. 2. 25. ~ 2026. 6. 8. (약 4개월)

붙임 2 'IP카메라 품질비교시험(보안 취약점 점검)' 결과

1 보안점검 종합결과 및 취약점 특이사항

□ 보안 취약점 점검 결과, 일부 제품은 사생활 유출 우려 있어

○ **(보안점검 종합결과)** 보안성 평가는 기기가 정보를 받아들이는 하드웨어부터 이를 처리하고 전달하는 통신망(네트워크), 내부를 제어하는 펌웨어, 사용자가 조작하는 앱, 그리고 제조사의 관리체계까지의 IP카메라의 보안체계를 점검함.

- 시험대상 IP카메라 10개 제품을 대상으로 보안 취약점을 점검*한 결과, 전반적으로 개선이 필요했음.

<보안성 평가 항목>

평가 항목		평가 내용
기기	하드웨어 (3)	SD카드 슬롯, 충전·USB 포트 등 IP카메라의 내·외부 물리적 인터페이스
	네트워크 (5)	IP카메라와 모바일 앱, 클라우드 서버 간 통신을 위한 연결 수단
	펌웨어 (11)	IP카메라 내부의 영상 처리, 시스템 제어 및 동작 로직 소프트웨어
모바일 앱 (15)		사용자가 IP카메라를 제어하고 설정할 수 있는 스마트폰 기반 애플리케이션
정책 관리 (3)		제조사의 보안 취약점 공개 정책, 보안 업데이트 정책, 개인정보 보호정책

※ 총 37개 항목(기기(하드웨어·네트워크·펌웨어) 19개, 모바일앱 15개, 정책 관리 3개 등)

<IP카메라 보안점검 종합평가 결과>

브랜드	모델명(상품명)	화소 수	보안 취약점 점검 종합평가 결과[주1)]	구입가격[원]
다후아	DH-H3B	300만 화소	★	35,000
로보뷰	GI-ROBOA7 (RoboView A7)	500만 화소	☆[주2)]	176,500
브이스타캠	VSTARCAM-800X	800만 화소	☆[주2)]	159,000
샤오미	MJSXJ16CM (C500 PRO)	500만 화소	★★	64,800
아이피타임	C500G	500만 화소	★	29,900
이글루	TSC-443P(S8)	400만 화소	★	119,000
타포	TC74	500만 화소	★★	69,800
파인뷰	K11	800만 화소	☆[주2)]	69,000
헤이홈	GKW-MC0511 (스마트 홈카메라 Pro+)	500만 화소	★★	72,900
하이크비전	CN-D1153G	500만 화소	★	73,000

<기호의 표시> ★★★ : 상대적 우수 ★★ : 양호 ★ : 보통 ☆ : 미흡

주1) 모바일 앱·기기(하드웨어, 네트워크, 펌웨어)·정책·관리 취약점 등 37개 항목 점검수행 결과, 취약점 특이사항 등을 종합하여 평가함.

주2) 보안 전문 인력의 고도화된 공격 시나리오 기반 점검 결과, 사생활 유출 가능 취약점 발견

○ **(점검 특이사항)** 시험대상 IP카메라 중 3개 제품은 사용자 인증절차가 미비한 취약점 등으로 인해 비인가자의 사진·영상 조회 및 원격 기능 강제 활성화 등 사생활 유출 우려가 있었음.

<이미지·영상 탈취 등 사생활 유출 가능성>

브랜드	모델명(상품명)	점검 결과
로보뷰	GI-ROBOA7(RoboView A7)	카메라 원격 기능 강제 활성화
브이스타캠	VSTARCAM-800X	타 사용자의 이미지 조회·탈취
파인뷰	K11	타 사용자의 이미지·영상 조회·탈취 및 카메라 조작

▣ 해당 취약점은 보안 전문 인력의 고도화된 공격 시나리오에 기반하여 도출된 결과로, 특정 수준 이상의 보안 기술과 도구를 보유한 공격자에 의해 악용될 가능성이 있음.

< 사생활 유출 가능 시나리오 상세 >

○ **(카메라 원격 기능 강제 활성화)** 로보뷰 제품은 기기 고유번호를 변경*하여 공격자와 같은 와이파이(Wi-Fi)에 연결된 타 사용자 IP카메라의 실시간 영상을 열람할 수 있었음.

* 기기 고유번호 변경 단계에서 소유자 ID 등을 함께 검증하는 절차가 필요

○ **(이미지·영상 탈취)** 브이스타캠, 파인뷰 2개 제품은 클라우드에 저장된 타 사용자 IP카메라 이미지·영상 조회 및 탈취가 가능했음.

- 브이스타캠 제품은 기기 고유번호를 변경하여 클라우드에 저장된 타 사용자 IP카메라의 이미지 조회 및 탈취가 가능했음.
- 파인뷰 제품은 클라우드 관리자 계정정보를 탈취하여 클라우드에 저장된 여러 사용자의 IP카메라의 이미지와 영상을 한 번에 조회하고 탈취하는 것이 가능했음.

○ **(실시간 영상 열람 및 제어)** 파인뷰 제품은 타 사용자 계정정보를 탈취하여 클라우드에 저장된 타 사용자 IP카메라의 실시간 영상을 열람하고 제어할 수 있었음.

2 기기·모바일 앱 보안 점검

□ 기기·모바일 앱 분야, 전반적으로 개선이 필요해

○ **(하드웨어)** 접속장치의 접근제어 등 하드웨어 접근 및 유출 방지 항목을 점검한 결과, 4개 제품*에서 접속장치**의 보안성 개선이 필요했음.

* 브이스타캠, 이글루, 파인뷰, 헤이홈

** UART 등 노출된 테스트 단자가 비활성화 되지 않아 내부 시스템 제어 및 직접적인 시스템 접근·정보 유출 위험이 있음

○ (**네트워크**) 네트워크 인증, 암호화, 데이터 보호 등 네트워크 보안을 점검한 결과, 8개 제품*에서 안전한 통신 프로토콜**(SSL/TLS 등)을 사용하지 않아 보안성 개선이 필요했음.

* 다후아, 로보뷰, 브이스타캠, 아이피타임, 이글루, 타포, 파인뷰, 하이크비전

** 데이터 송수신 과정을 암호화하여 전송하는 보안 통신 규격으로, 미사용 시 데이터가 유출될 위험이 있음

○ (**펌웨어**) 펌웨어 보호, 인증, 취약점 등 전반적인 시스템 보안을 점검한 결과, 모든 제품이 펌웨어 보안 설정*이 취약해 기기의 내부 보안 매커니즘이 외부에 노출될 우려가 있어 개선이 필요했음.

* 보안에 취약한 불필요한 명령어 및 기능이 있거나 펌웨어의 보안 설정이 제대로 적용되지 않음.

○ (**모바일 앱**) 전 제품에서 역설계 방지 기법* 취약, 5개 제품**에서는 안전한 패스워드 정책*** 미적용으로 개선이 필요했음.

* 완성된 소프트웨어나 앱의 소스코드를 분석·복원해 원래의 설계도, 구동 로직 획득을 차단하는 보안 기술

** 다후아, 브이스타캠, 샤오미, 아이피타임, 타포

*** 패스워드 입력 시 대·소문자, 숫자, 특수문자 중 3조합 8자리 이상 또는 2조합 10자리 이상 설정 등 패스워드 강도에 대한 안전한 정책이 적용되지 않아 보안상 미흡함.

3 정책·관리 보안 점검

□ 정책·관리 분야, 제품별 운영 중인 정책에 차이 있어

○ (**정책·관리**) 취약점 관리 정책 등 정책·관리 분야를 점검한 결과, 5개* 제품은 취약점 발견 시 신고·처리 절차가 부재했고, 6개** 제품은 펌웨어에 대한 보안 업데이트 지원 기간의 확인이 불가능해 취약한 상태로 기기를 운용할 위험이 있어 개선이 필요했음.

* 로보뷰, 아이피타임, 이글루, 파인뷰, 헤이홈

** 로보뷰, 브이스타캠, 아이피타임, 이글루, 파인뷰, 헤이홈

붙임 3 조사대상 제품

□ 소비자 설문조사*, 온라인 쇼핑몰 판매** 순위 등을 기준으로 10개 브랜드 선정

* 최근 2년 이내에 IP카메라를 구입 및 사용한 경험이 있는 소비자 600명 대상(한국소비자원, 2025. 12.)

** 3개 쇼핑몰(다나와, 11번가, 쿠팡) 판매 순위를 종합

○ 브랜드별 판매량 및 기능*을 고려하되, 소비자 점유율이 높은 5개 제품은 품질도 추가로 평가함.

* 최근 2년 이내 출시된 모델, 해상도 300만 화소 이상, 무선연결 등

<점검·시험평가 대상 제품>

브랜드	모델명(상품명)	해상도	가격*[원]	비고
샤오미	MJSXJ16CM (C500 PRO)	5MP(500만)	64,800	보안 점검 · 품질 평가
아이피타임	C500G	5MP(500만)	29,900	
이글루	TSC-443P(S8)	4MP(400만)	119,000	
타포	TC74	5MP(500만)	69,800	
헤이홈	GKW-MC0511 (스마트 홈카메라 Pro+)	5MP(500만)	72,900	
다후아	DH-H3B	3MP(300만)	35,000	보안 점검
로보뷰	GI-ROBOA7 (RoboView A7)	5MP(500만)	176,500	
브이스타캠	VSTARCAM-800X	8MP(800만)	159,000	
파인뷰	K11	8MP(800만)	69,000	
하이크비전	CN-D1153G	5MP(500만)	73,000	

* 2026년 2월 온·오프라인 구입가 기준, 구입처·수량 및 구입 시기에 따라 상이할 수 있음.
가격은 SD카드 등 부가 액세서리를 제외한 단품 기준 금액임.

붙임 4-1 **사용자 보안 수칙**

안전한 IoT 사용을 위한 사용자 보안 수칙



01 구매 및 설치 시 IoT 기기를 사용하기 전에 꼭 확인하세요.

1 기본 비밀번호 즉시 변경
- 초기 제공 비밀번호를 그대로 사용하지 않기
- 영문 대소문자·숫자·특수문자를 조합해 설정

2 공식 앱만 설치
- 구글 플레이, 앱 스토어 등 공식 배포처 이용
- 출처가 불분명한 앱은 설치하지 않기

3 안전한 공유기에 연결
- WPA3 또는 WPA2 등 안전한 무선 보안 방식 사용
- 공유기 관리자 비밀번호도 함께 변경

4 보안 인증 제품 확인
- KISA IoT 보안인증 등 여부 확인
- 신뢰할 수 있는 제조사의 제품 선택

02 사용 중 평소 사용하면서 습관처럼 점검하세요.

5 최신 보안 업데이트 적용
- IoT 기기, 연동 앱을 최신 버전으로 유지
- 자동 업데이트 기능 켜 두기

6 저장 데이터 안전하게 관리
- 필요 없는 영상과 데이터는 정기적으로 삭제

7 2단계 인증 설정 및 접속 알림 확인
- 의심스러운 접속이 있으면 비밀번호 즉시 변경
- 비밀번호 외에 추가 인증 수단을 함께 사용

8 사용하지 않는 원격 접속 끄기
- 사용하지 않는 원격 접속 기능은 꺼 두기
- 외부 공개 설정은 필요한 범위로 제한

03 중고 거래 및 폐기 시 마지막으로 한번 더 확인하세요.

9 중고 거래 전 공장 초기화
- 계정 연동을 해제하고 저장 영상과 개인 설정 삭제
- 공장 초기화를 확인한 뒤 중고 거래 진행

10 폐기 시
- 기기 내 저장된 영상·개인정보 완전 삭제
- 저장매체가 있으면 초기화 후 폐기

작은 보안 습관이 해킹과 개인정보 유출을 예방합니다.

과학기술정보통신부 Ministry of Science and ICT | 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY | 한국소비자원 Korea Consumer Agency

붙임 4-2 **제조 · 유통사 보안 수칙**

안전한 IoT 보급을 위한 제조·유통사 보안 수칙



01 설계 및 개발 처음부터 보안을 적용하여 안전한 IoT 제품을 설계하세요.

1 기본 계정·비밀번호 정책 강화
- 제품마다 서로 다른 초기 비밀번호 적용
- 처음 사용할 때 비밀번호를 반드시 변경하도록 설정

2 전용 앱·펌웨어 위·변조 방지
- 전용 앱의 위·변조 탐지 및 방지 기능 적용
- 펌웨어의 전자서명을 검증하고 불법 시험·변조 여부 확인

3 안전한 통신 및 암호화 방식 적용
- 전송 계층 보안(TLS) 1.2 이상, WPA3 지원
- 취약하거나 지원이 종료된 암호·통신 방식 사용 금지

4 불필요한 서비스·기능 비활성화
- 출하 제품의 개발·점검용 접속 기능 제거 또는 비활성화
- 사용하지 않는 외부 공개 기능·경로 비활성화

02 검증 및 인증 출하 전 보안 검증을 빠짐없이 수행하세요.

5 안전한 업데이트 체계 구축
- 보안 업데이트를 안전하고 신속하게 배포하는 체계 운영
- 전자서명이 확인된 펌웨어만 설치되도록 제한

6 보안 인증 및 표준 준수
- 제품에 해당하는 보안인증을 출하 전에 획득
- 국내외 보안 표준의 요구사항 충족

03 제조자 개발생산(ODM) 제품 유통 시 제품을 유통하거나 변경할 때도 보안을 유지하세요.

7 도입 및 맞춤 변경 시 보안확인
- 도입하는 하드웨어·소프트웨어의 보안취약점 존재 여부 점검
- 보안 패치·업데이트 지원 여부 점검
- 보안설정을 임의로 낮추지 않기
- 자체 변경한 프로그램과 설정에 대해 보안점검 수행

8 외부 서비스 연동 시 보안 검증
- 외부 서비스·클라우드 연동 구간 보안점검
- 연동 구간 인증·권한 관리 검증

04 운영 및 지원 관리 출시 이후에도 책임 있게 관리하세요.

9 지속적인 취약점 관리
- 공개 취약점을 확인한 후 보안업데이트를 신속히 배포
- 제품 지원 기간 및 종료기간 안내
- 취약점 신고 창구 등 대응체계 마련

안전한 제품과 책임 있는 유통이 신뢰받는 IoT 시장을 만듭니다.

과학기술정보통신부 Ministry of Science and ICT | 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY | 한국소비자원 Korea Consumer Agency

붙임 5 보안 점검항목

번호	구분		항목
①	기기	하드웨어	물리적 접근제어
②			인터페이스 존재 여부
③			인터페이스 접근제어
④		네트워크	안전한 통신 프로토콜 및 서비스 사용
⑤			전송 데이터 암호화
⑥			송수신 데이터 변조
⑦			불필요한 서비스
⑧			취약한 인증정보 사용
⑨		펌웨어	펌웨어 추출 시 암호화
⑩			중요정보 출력
⑪			보안 설정
⑫			안전한 커널 및 운영체제 사용
⑬			취약한 라이브러리
⑭			펌웨어 무결성 검증

번호	구분		항목
⑮	기기	펌웨어	중요정보 평문 저장
⑯			불필요한 파일
⑰			부족한 입력 및 출력 검증
⑱			디버깅 페이지 사용
⑲			취약한 인증서 사용
⑳	모바일 앱		초기 인증정보 설정
㉑			안전한 패스워드 정책
㉒			계정 잠금 임계값 설정
㉓			인증 실패 정보 제공
㉔			전송 데이터 암호화
㉕			역공학 방지 기법 적용
㉖			세션 관리
㉗			개인정보 및 개인위치정보 수집 및 활용에 대한 동의
㉘			과도한 권한 설정

번호	구분	항목
㉙	모바일 앱	중요정보 평문 저장
㉚		하드코딩된 중요정보
㉛		불충분한 인증 및 인가
㉜		부족한 입력 및 출력 검증
㉝		취약한 라이브러리
㉞		안전하지 않은 딥링크
㉟	정책 관리	제조사 취약점 관리 정책
㊱		보안 업데이트 제공
㊲		개인정보 보호정책

※(국내) IoT 보안인증(KISA), 국정원 보안요구사항, 행안부 고시(모바일 앱, 서버) (국외) EN 303 645(ETSI), OWASP(ISTG(IoT보안), MAS(모바일보안)), OWASP 모바일(TOP10)) 등 참고

붙임 6 제품 사진

브랜드	샤오미	아이피타임	이글루	타포	헤이홈
모델명	MJSXJ16CM	C500G	TSC-443P	TC74	GKW-MC0511
제품사진					
브랜드	다후아	로보뷰	브이스타캠	파인뷰	하이크비전
모델명	DH-H3B	GI-ROBOA7	VSTARCAM-800X	K11	CN-D1153G
제품사진					