

무선공유기 펌웨어 보안점검

문서 종류 지엔 무료 제품 보안점검 · 요약 리포트

분석일 분석일 2026-09-10



© 2026 ZIEN, Inc. All Rights Reserved.

본 문서는 실물 기기가 아닌 **영업용 샘플**입니다.

1. 보안점검 요약

1.1 점검 개요

펌웨어 이미지를 정적 분석하여 구성요소와 알려진 취약점을 확인하였습니다.

항목	내용
제품	모델명 비공개
펌웨어	파일명 비공개
아키텍처	ARM · AArch64
펌웨어 크기	42.41 MB
분석일	2026-09-10
분석 범위	펌웨어 정적 분석 · 구성요소 식별(SBOM)

분석 항목

항목	내용	결과
SBOM 분석	펌웨어에서 HW·SW·AI 모델 구성요소를 식별하고 알려진 취약점(CVE) 제시	2.1
취약점 분석	펌웨어를 분해하여 패스워드·암호화·바이너리 하드닝을 항목별로 판정	2.2

1.2 적용 규제와 마감

이 제품은 무선기기이므로 카메라·산업기기에 적용되는 EU 기계류 규정 대상이 아닙니다. 대신 무선기기지침(Radio Equipment Directive, RED)의 사이버보안 요구사항이 적용됩니다.

규제	적용	마감
CRA 제14조 · 취약점 보고 의무	해당	시행일 2026-09-11
CRA 부속서 I · 본 의무	해당	2027-12-11 · D-457
RED 제3조(3)(d)(e)(f) · EN 18031-1/2/3	해당	2025-08-01부로 시행 중

CRA 제14조는 2026-09-11부터 시행됩니다. 무선기기 사이버보안 요구사항(EN 18031)은 이미 1년 넘게 시행 중이며, 이 시점에 유통 중인 제품이라면 이미 적용 대상입니다.

CRA 부속서 I 충족도

20 요건 총계	1 충족	3 미충족	16 범위 밖
--------------------	----------------	-----------------	-------------------

이번 분석은 SBOM과 펌웨어 정적 바이너리 점검 두 가지를 통해 직접 근거를 달 수 있는 항목만 충족·미충족으로 판정하였습니다. 상세한 항목별 근거는 2.3에 기재하였습니다.

1.3 결과 요약

BOM 결과

400 식별 구성요소	2 하드웨어	397 소프트웨어	1 AI 모델	1,899 CVE
-----------------------	------------------	---------------------	-------------------	---------------------

취약점 분석 결과

0 패스워드 취약점	1 암호화 취약점	84 하드닝 취약 바이너리	3 익스플로잇 후보
----------------------	---------------------	--------------------------	----------------------

전체 취약점 심각도 분포 · 총 1,900건

Critical		712
High		562
Medium		557
Low		69

주요 발견 사항

발견	등급	문제	위치
ProFTPD 1.3.4 · CVE-2019-12815	Critical	mod_copy로 임의 파일 복사. 공개 익스플로잇 코드(PoC) 존재, 익스플로잇 예측 점수(EPSS) 57.6%	2.1.2
OpenSSL 1.0.2	High	2019년 지원 종료 계열. 암호 통신 기반 구성요소	2.1.3
BIN-F · 익스플로잇 후보	유력	스택 오버플로우 위험 함수 호출 557건(전체 중 최다), RELRO 미적용 — 하드닝 프로파일상 가장 취약	2.2.1
BIN-A · 익스플로잇 후보	유력	OS 명령·인젝션 위험 함수 호출 45건(전체 중 최다)	2.2.1
hostapd 2.7 · CVE-2019-9494	High	WPA3 SAE 핸드셰이크 캐시 기반 사이드채널 → 패스워드 복구 가능(Wi-Fi 인접 공격자)	2.1.2
OpenVPN 2.4.11 · CVE-2020-15078	Medium	auth-gen-token 기능의 인증 우회·정보 노출	2.1.2

전문가 소견

가장 시급한 항목은 ProFTPD의 mod_copy 취약점(CVE-2019-12815)입니다. CVSS 9.8에 공개 PoC까지 존재해, FTP 서비스가 외부에 노출되어 있다면 SITE CPFR·CPTO 명령만으로 임의 파일을 웹 실행 경로에 복사해 원격 코드 실행으로 이어질 수 있어 최우선 조치 대상입니다.

나머지 CVE 기반 항목은 조건부입니다. OpenSSL 1.0.2는 2019년 지원이 종료되어 신규 취약점에 패치를 받지 못하는 상태이고, hostapd·wpa_supplicant 2.7은 WPA3 SAE 핸드셰이킹의 사이드채널 결함(CVE-2019-9494)으로 Wi-Fi 인접 공격자에게 패스워드가 노출될 수 있습니다(WPA2-PSK만 사용한다면 해당 없음). OpenVPN 2.4.11의 auth-gen-token 인증 우회(CVE-2020-15078)는 이 기능을 켜둔 경우에만 영향을 받습니다.

BIN-F는 별도 CVE 없이 정적 지표만으로 추정된 후보입니다. 스택 오버플로우 위험 함수 호출이 557건으로 가장 많고 RELRO도 미적용되어 있어 하드닝 프로파일상 가장 취약하며, 실행 경로가 외부 입력에 실제로 도달하는지는 검증이 필요합니다.

ProFTPD·OpenSSL·OpenVPN은 취약점 존재가 확인되는 대로 패치가 필요하고, hostapd·wpa_supplicant는 WPA3 사용 여부, BIN-F는 코드 도달 가능성 확인이 우선입니다.

분석: 지엔 · 2026-09-10

2. 보안점검 결과

2.1 BOM

BOM 분석으로 펌웨어에서 하드웨어 부품(HW)·소프트웨어 구성요소(SW)·온디바이스 AI 모델을 하나의 목록으로 식별 하였습니다. 총 400건입니다.

2.1.1 BOM 식별 결과

유형	건수	식별 방법
SW · 패키지 DB 등록	359	펌웨어 내 패키지 관리자 메타데이터(control 파일)를 파싱하여 식별. 가장 신뢰도 높음
SW · 바이너리 지문(교차 검증)	2	패키지 관리자 메타데이터와 바이너리 지문 양쪽에서 동시 확인 (busybox, curl)
SW · 바이너리 지문 단독	2	펌웨어 내 패키지 관리자 메타데이터가 없어 바이너리 지문만으로 식별 (openssl, proftpd)
SW · YARA 패턴 매칭	34	버전 미상. 문자열 시그니처로만 존재 확인
HW · 하드웨어 역추론	2	펌웨어 내 드라이버·커널 모듈 문자열에서 역추론(HBOM)
AI · 온디바이스 모델	1	모델 파일 헤더·확장자와 로딩 바이너리의 참조 문자열로 확인
합계	400	

주요 SBOM

이름	버전	근거
openssl	1.0.2	바이너리 지문 식별 · 지원 종료(2019-12) 계열. TLS·VPN 기능의 암호 기반. CVE 214건
proftpd	1.3.4	바이너리 지문 식별 · CVE-2019-12815 영향 버전 대역. CVE 17건
curl	7.79.1	패키지 DB·바이너리 지문 교차검증 · HTTP 클라이언트 라이브러리. CVE 138건
busybox	1.34.1	패키지 DB·바이너리 지문 교차검증 · 코어 유틸리티 모음. CVE 28건
dnsmasq	2.83	패키지 DB 등록 · DNS·DHCP 서비스. CVE 29건
openvpn	2.4.11	패키지 DB 등록 · VPN 클라이언트·서버. CVE 23건
strongswan	5.8.2	패키지 DB 등록 · IPsec VPN 데몬. CVE 20건

이름	버전	근거
hostapd	2.7	패키지 DB 등록 · Wi-Fi AP 데몬. CVE 19건
wpa_supplicant	2.7	패키지 DB 등록 · Wi-Fi 인증 클라이언트. CVE 18건
iptables	1.4.21	패키지 DB 등록 · 방화벽 규칙 관리. CVE 3건

HBOM

부품	역할	근거	신뢰도
Broadcom BCM49xx 계열	메인 SoC	rootfs 내 드라이버·펌웨어 blob 문자열	확인됨
Broadcom BCM436xx 계열	WiFi · 블루투스	rootfs 내 드라이버·펌웨어 blob 문자열, 신뢰도 75%	확인됨(추정 포함)

이 샘플에서는 칩셋 모델명을 계열 단위로만 표기하였습니다. 실제 리포트에서는 전체 모델명을 제공합니다.

AI BOM

항목	내용
모델 파일	파일명 비공개
모델 아키텍처	MobileNetV2 기반 트래픽 분류 모델 (TFLite, int8 양자화, 약 1.1MB)
용도	트래픽 분류 · 이상행동 탐지

2.1.2 주요 CVE

실제 설치가 확인된 버전 기준으로 재선별한 결과입니다. 버전이 확정되지 않은 후보까지 포함한 1.3의 집계와는 기준이 다릅니다.

구성요소	CVE 총합	Critical	High	Medium	Low
openssl 1.0.2	214	11	74	116	13
curl 7.79.1	138	28	48	53	9
dnsmasq 2.83	29	3	12	10	4
busybox 1.34.1	28	3	18	6	1
openvpn 2.4.11	23	4	11	6	2
strongswan 5.8.2	20	2	11	6	1
hostapd 2.7	19	2	9	6	2
wpa_supplicant 2.7	18	2	6	9	1

구성요소	CVE 총합	Critical	High	Medium	Low
proftpd 1.3.4	17	1	11	4	1
iptables 1.4.21	3	0	1	1	1
합계	509	56	201	217	35

검토가 시급한 CVE

구성요소	CVE	CVSS	EPSS	공개 PoC	영향
proftpd 1.3.4	CVE-2019-12815	9.8	57.6%	있음(고품질)	mod_copy로 임의 파일 복사 → 원격 코드 실행 가능
openvpn 2.4.11	CVE-2020-15078	5.3	—	있음	auth-gen-token 기능의 인증 우회·정보 노출
hostapd 2.7	CVE-2019-9494	7.7	—	있음	WPA3 SAE 핸드셰이크 캐시 기반 사이드채널 → 패스워드 복구 가능(Wi-Fi 인접 공격자, wpa_supplicant 2.7 동일 영향)

2.1.3 지원 종료 구성요소

구성요소	현재	지원 상태
openssl	1.0.2	지원 종료 (2019-12)
proftpd	1.3.4	사실상 종료. 최신 안정 계열은 1.3.9

지원이 종료된 구성요소는 신규 취약점이 발견되어도 공식 패치를 받을 수 없습니다.

2.1.4 전문가 소견

핵심 취약점은 openssl 1.0.2, proftpd 1.3.4, hostapd 2.7, openvpn 2.4.11입니다. openssl 1.0.2는 2019년 12월 지원이 종료된 계열로 214건의 CVE가 누적되어 있으며, proftpd 1.3.4는 mod_copy를 통한 임의 파일 복사 취약점(CVE-2019-12815, CVSS 9.8)의 영향을 받습니다. hostapd 2.7(및 wpa_supplicant 2.7)은 WPA3 SAE 핸드셰이크의 캐시 기반 사이드채널 취약점(CVE-2019-9494, CVSS 7.7)의 영향을 받으며, openvpn 2.4.11은 auth-gen-token 기능의 인증 우회 취약점(CVE-2020-15078, CVSS 5.3)의 영향을 받습니다.

네 구성요소 모두 실제 운영 환경에서의 영향 여부를 검토해야 하는 수준입니다. openssl은 지원 계열로의 교체 우선순위를 높이고, proftpd는 외부 접근 가능한 인터페이스에서 구동되는지 확인해야 합니다.

분석: 지엔 · 2026-09-10

2.2 펌웨어 점검

펌웨어에 대한 점검결과는 아래와 같습니다.

바이너리 이름 표기. 이 샘플에서는 벤더 고유 바이너리 이름을 BIN-A ~ BIN-F로 표기하였습니다. 실제 리포트에서는 파일 시스템상의 실제 파일명과 경로로 제공합니다.

패스워드 · 인증

항목	판정	발견 내용
하드코딩 자격증명	미발견	하드코딩된 계정·비밀번호가 확인되지 않았습니다

암호화

항목	판정	발견 내용
루트 CA 인증서 서명 알고리즘	미흡	ca-certificates.crt에 포함된 ACCVRAIZ1 루트 인증서가 sha1WithRSAEncryption으로 서명됨. SHA-1은 서명 알고리즘으로 더 이상 권장되지 않음

인증서 관리 주기(만료일 재확인, 취약한 서명 알고리즘 인증서 교체)를 정기적으로 점검하는 절차가 필요합니다.

바이너리 하드닝

전체 바이너리 84개를 컴파일 보호 옵션(RELRO, NX, CANARY, PIE, 심볼 스트립) 기준으로 점검하였습니다. 다음은 위험 함수 호출 상위 6개 바이너리입니다.

바이너리	OS 명령·인젝션 함수 호출	스택 오버플로우 함수 호출	RELRO	NX	CANARY	PIE
BIN-A	45	26	부분	적용	미적용	미적용
BIN-B	21	82	부분	적용	미적용	미적용
BIN-C	21	54	부분	적용	미적용	미적용
BIN-D	20	84	부분	적용	미적용	미적용
BIN-E	15	37	부분	적용	미적용	미적용
BIN-F	0	557	미적용	적용	미적용	미적용

84개 바이너리 전부에서 CANARY와 PIE가 적용되어 있지 않습니다. NX(실행 방지)만 전 바이너리에 일괄 적용되어 있습니다.

BIN-A ~ BIN-F는 실제 파일명을 의도적으로 마스킹한 표기입니다. 실제 리포트에서는 파일시스템상의 실제 경로로 제공됩니다.

2.2.1 익스플로잇 후보 · 3 건

#	대상	판정 근거	우선순위
1	BIN-F	스택 오버플로우 위험 함수 호출 557건(전체 중 최다), RELRO 미적용(다른 5개는 부분 적용) — 하드닝 프로파일상 가장 취약	유력
2	BIN-A	OS 명령·인젝션 위험 함수 호출 45건(전체 중 최다) — 커맨드 인젝션 경로 가능성	유력
3	BIN-D	스택 오버플로우 위험 함수 호출 84건(BIN-F 다음으로 최다)	확인 필요

2.2.2 전문가 소견

패스워드는 하드코딩된 계정·비밀번호가 발견되지 않았습니다. 암호화는 루트 CA 인증서가 SHA-1으로 서명되어 있어 미흡 수준이며, 바이너리 하드닝은 84개 전부에서 CANARY·PIE가 미적용된 상태입니다. 그중 BIN-F는 스택 오버플로우 위험 함수 호출이 557건으로 가장 많고 RELRO도 미적용되어 있으며, BIN-A는 명령 인젝션 위험 함수 호출이 45건으로 가장 많고, BIN-D는 스택 오버플로우 위험 함수 호출이 84건으로 BIN-F 다음으로 많아 세 바이너리 모두 익스플로잇 후보로 분류하였습니다.

이번 점검은 펌웨어 파일 기준의 정적 분석으로, 세 바이너리의 실행 경로가 외부 입력에 실제로 도달하는지는 검토가 필요한 수준입니다. SHA-1 인증서 교체와 BIN-F·BIN-A·BIN-D의 하드닝 옵션 적용·취약 함수 교체를 우선 검토해야 합니다.

2.3 규제 · EU CRA

CRA Annex I 정의된 제품의 필수 사이버 보안 요구사항(제조 시 설계 보안 기준 등 약 20여 개 세부 조항)을 이번 분석 결과에 대조하였습니다. SBOM과 정적 바이너리 점검 두 소스로 직접 근거를 댈 수 있는 항목만 충족·미충족으로 판정하였고, 근거가 없는 항목은 전부 범위 밖으로 남겼습니다.

구분	조항	요건	평가결과	판단 근거
제1부	I-1	알려진 취약점 없이 출시	미충족	proftpd CVE-2019-12815(CVSS 9.8), openssl 대량 CVE(214건) 미조치
제1부	I-2	기본 설정이 안전할 것	범위 밖	하드코딩 자격증명은 미발견이나, 기본 서비스 활성화 여부는 기기 동작 확인 필요
제1부	I-3	보안 업데이트로 수정 가능	미충족	openssl 1.0.2, proftpd 1.3.4 지원 종료 구성요소가 상류 패치를 받지 못함
제1부	I-4	무단 접근 방지	범위 밖	서비스 접근 통제는 기기 동작 확인 필요
제1부	I-5	저장·전송 데이터 기밀성	범위 밖	기기 동작 확인 필요
제1부	I-6	데이터 무결성	범위 밖	정적 분석으로 판단 불가
제1부	I-7	최소 데이터 처리	범위 밖	정적 분석으로 판단 불가
제1부	I-8	가용성 보호	범위 밖	정적 분석으로 판단 불가
제1부	I-9	공격면 최소화	범위 밖	정적 분석만으로는 네트워크 노출 여부를 판단하기 어려워 기기 동작 확인이 필요함
제1부	I-10	사고 영향 완화	범위 밖	기기 동작 확인 필요
제1부	I-11	보안 이벤트 기록	범위 밖	로그 기능 존재 여부는 확인하였으나 기록 내용은 기기 동작 확인 필요
제1부	I-12	데이터 삭제 기능	범위 밖	정적 분석으로 판단 불가
제2부	II-1	SBOM 작성·유지	충족	실제 CycloneDX 1.6 SBOM 파일 존재(400개 구성요소)
제2부	II-2	취약점을 지체 없이 해결	미충족	proftpd, openssl 미조치
제2부	II-3	정기 보안 시험	범위 밖	시험 이력 확인 불가
제2부	II-4	수정한 취약점 정보 공개	범위 밖	보안 권고문 게시 여부 확인 불가
제2부	II-5	CVD 정책 수립	범위 밖	정책 문서 게시 여부 확인 불가
제2부	II-6	신고 연락처 공개	범위 밖	security.txt 등 게시 여부 확인 불가

구분	조항	요건	평가결과	판단 근거
제2부	II-7	안전한 업데이트 배포	범위 밖	업데이트 서명 검증 로직은 이번 분석에서 다루지 않음
제2부	II-8	보안 패치 분리 배포	범위 밖	배포 채널 확인 필요

본 문서는 실물 기기가 아닌 영업용 샘플입니다.

주식회사 지엔 · ZIEN · 무료 제품 보안점검 · 2026-09-10