

Software Bill of Materials (SBOM) — Garbi Sein

Dit document geeft een overzicht van de software-componenten die in de firmware van Garbi Sein zijn verwerkt, conform Bijlage I, Deel II van de EU Cyber Resilience Act (Verordening (EU) 2024/2847). Het is een mensleesbare weergave; zie [hoofdstuk 6](#) voor de status van een machineleesbaar formaat.

1. Product

Product	Garbi Sein
Model	Garbi Sein v1
Firmwareversie waarop dit document betrekking heeft	1.4.0
Hardwareplatform	DFRobot "Beetle ESP32-C6" (module DFR1117, chip ESP32-C6FH4)
Fabrikant firmware	Eagle Software Consultancy B.V., KVK 98050516

2. Eigen firmwarecode

Component	Garbi Sein-firmware
Auteursrecht	Eagle Software Consultancy B.V.
Licentie	Propriëtair — niet onder een open-source licentie gepubliceerd
Rol	Applicatielogica: afvalschema ophalen en tonen, ledaansturing, webportaal voor instellingen, OTA-update-client

3. Directe software-afhankelijkheden (libraries)

Deze libraries worden als broncode meegecompileerd in de firmware en zijn dus onderdeel van het uitgeleverde binary. Versies zijn vastgepind en hieronder weergegeven zoals daadwerkelijk gebruikt in deze firmware.

COMPONENT	VERSIE	LICENTIE	LEVERANCIER/BRON	ROL IN DE FIRMWARE
ArduinoJson	7.4.3	MIT	Benoit Blanchon	Parsen van afvalschema-API-responses en OTA-versie-informatie (JSON)
WiFiManager	2.0.17	MIT	tzapu / tablatronix	Captive-portal wifi-provisioning bij eerste installatie
Adafruit NeoPixel	1.15.5	LGPL-3.0	Adafruit Industries	Aansturing van het WS2812-statusledje

4. Firmwareframework en platformlaag

COMPONENT	VERSIE	LICENTIE	LEVERANCIER/BRON	ROL
Arduino-ESP32 core	3.3.11	LGPL-2.1-or-later	Espressif Systems (pioarduino-distributie)	Arduino-API-laag (<code>WiFi</code> , <code>HTTPClient</code> , <code>NetworkClientSecure</code> /TLS, <code>WebServer</code> , <code>ESPmDNS</code> , <code>Preferences</code> , <code>HTTPUpdate</code>) bovenop ESP-IDF
ESP-IDF (gebundeld in de Arduino-core)	v5.5.5	Apache-2.0 (met onderdelen onder eigen licenties, o.a. mbedTLS: Apache-2.0)	Espressif Systems	Onderliggende chip-drivers, TCP/IP-stack (lwIP), TLS-stack (mbedTLS), FreeRTOS, bootloader

De exacte sub-versies van individuele ESP-IDF-componenten (bijvoorbeeld de precieze mbedTLS- of lwIP-patch-versie) worden niet los bijgehouden door dit project; ze liggen vast door de pin op ESP-IDF v5.5.5 hierboven. Bij een kwetsbaarheid in een van die componenten is ESP-IDF v5.5.5 het aanknopingspunt om te bepalen of deze firmware geraakt wordt.

5. Niet in deze SBOM opgenomen

- **Build-gereedschap** (esptoolpy, scons, de compiler-toolchain, etc.): deze worden gebruikt om de firmware te bouwen maar maken geen deel uit van de uiteindelijke firmware-binary op het apparaat, en vallen daarmee buiten de reikwijdte van een product-SBOM.
- **Root-CA-certificaten** (`src/CertBundle.h`): dit zijn publieke, niet-geheime configuratiegegevens (vertrouwde stamcertificaten), geen uitvoerbare software-component.

6. Kwetsbaarhedenbeheer

Laatste kwetsbaarhedenscan van bovenstaande componenten	2026-09-17
Gebruikt hulpmiddel	Voor ESP-IDF/mbedtls/cJSON (§4): Espressif's officiële ESP-IDF Security Dashboard (<code>esp-idf-sbom</code> , automatisch gekruist tegen de NVD, dagelijks bijgewerkt) - de scanresultaten voor exact v5.5 zijn rechtstreeks opgehaald. Voor ArduinoJson/WiFiManager/Adafruit NeoPixel (§3, geen onderdeel van dat dashboard): handmatige controle van GitHub Security Advisories en publieke CVE-databases per component.
Openstaande bevindingen	4 CVE's gerapporteerd voor ESP-IDF v5.5.5, alle vier gerelateerd aan cJSON - zie toelichting hieronder waarom deze niet van toepassing zijn op deze firmware. Voor ArduinoJson: één historische CVE (CVE-2015-4590, versies vóór 4.5) - niet van toepassing , dit project gebruikt 7.4.3. Voor WiFiManager en Adafruit NeoPixel: geen bekende CVE's/advisories gevonden.

Toelichting bij de 4 cJSON-gerelateerde bevindingen

Beoordeeld tegen de daadwerkelijk gecompileerde firmware (nagegaan via de gelinkte symbolen in het binary, niet aangenomen):

- **cJSON (4 CVE's, `cJSONUtils_ApplyPatches` / `cJSON_Compare` / `print_string_ptr` -gerelateerd): niet van toepassing.** cJSON wordt (transitief) meegecompileerd, maar het gecompileerde firmware-binary bevat alleen de functie `cJSON_Delete` - geen van de daadwerkelijk kwetsbare functies is aanwezig. Deze applicatie gebruikt bovendien uitsluitend ArduinoJson voor eigen JSON-verwerking (zie §3), nooit cJSON rechtstreeks.

Kanttekening bij deze beoordeling: dit is een handmatige, eenmalige analyse op basis van gelinkte symbolen en configuratie, geen doorlopende geautomatiseerde SCA-pipeline. Een symbool dat aanwezig is, bewijst dat een functie *kan* worden aangeroepen, niet noodzakelijk dát dit binnen deze firmware ook daadwerkelijk met aanval-gecontroleerde invoer gebeurt (en omgekeerd sluit de afwezigheid van een symbool misbruik via een aanroeppad dat deze analyse niet heeft gevonden niet volledig uit).

Zie het [Coordinated Vulnerability Disclosure-beleid](#) voor hoe kwetsbaarheden in deze firmware of haar afhankelijkheden gemeld kunnen worden.

7. Licentiecompatibiliteit

Alle bovenstaande licenties (MIT, LGPL-2.1-or-later, LGPL-3.0, Apache-2.0) zijn toegestaan voor gebruik in een gesloten, niet-open-source eindproduct zoals deze firmware, mits aan de voorwaarden van de betreffende licentie wordt voldaan (met name de LGPL-onderdelen: broncode van eventuele *wijzigingen* aan de LGPL-gelicentieerde

library zelf moet, indien gemaakt, beschikbaar worden gesteld — deze firmware gebruikt Adafruit NeoPixel en de Arduino-ESP32 core ongewijzigd).

8. Onderhoud van dit document

Deze SBOM wordt bijgewerkt bij elke firmware-release waarin een afhankelijkheid wordt toegevoegd, verwijderd of van versie wisselt.

Laatst bijgewerkt: 2026-09-17
