

Productveiligheidsinformatie en ondersteuningsverklaring — Garbi Sein

Deze informatie wordt gepubliceerd conform Bijlage II van de EU Cyber Resilience Act (Verordening (EU) 2024/2847) en vult de [Gebruikershandleiding](#) aan met specifiek beveiligings- en ondersteuningsgerelateerde informatie.

1. Fabrikant

Naam	Eagle Software Consultancy B.V.
Adres	Kanteklaarpad 11, 3813 KR Amersfoort, Nederland
KVK-nummer	98050516
Algemeen contact	info@eaglesc.nl
Beveiligingsmeldingen	security@eaglesc.nl
Website	www.eaglesc.nl

2. Beoogd gebruik

Garbi Sein is een wifi-verbonden notificatielampje voor thuisgebruik, bedoeld om de bewoner eraan te herinneren welke afvalcontainer op welke dag aan de straat gezet moet worden, op basis van het ophaalschema van de door de gebruiker gekozen afvalinzamelaar. Het apparaat is bedoeld voor gebruik binnenshuis, aangesloten op het eigen wifi-netwerk van de gebruiker, en heeft geen beveiligings-, toegangscontrole- of veiligheidskritische functie.

3. Bekende en redelijkerwijs te verwachten vormen van oneigenlijk gebruik

- Gebruik buiten het beoogde binnenshuis-gebruik** (vocht, directe regen/zon): kan de elektronica beschadigen; niet voorzien als gebruiksscenario.
- Delen van het apparaat-ID of de netwerkn naam met derden**: het apparaat-ID identificeert een individueel apparaat maar geeft op zichzelf geen toegang tot de instellingen; het biedt geen extra bescherming en hoeft niet geheim gehouden te worden, maar wordt ook niet gebruikt als authenticatiemiddel.
- Het apparaat bereikbaar maken vanaf buiten het eigen thuisnetwerk** (bijvoorbeeld door portforwarding op de router): dit wordt **afgeraden**. De instellingenpagina is ontworpen voor gebruik binnen

een vertrouwd thuisnetwerk (HTTP, geen TLS-terminatie op het apparaat zelf) - zie punt 5 hieronder.

- **Het instellingenwachtwoord niet meteen instellen:** het instellen van een wachtwoord is verplicht - nieuwe apparaten vragen het al tijdens de eerste installatie af, en het apparaat weigert elke instellingenwijziging totdat er een wachtwoord is ingesteld (zie punt 5). Alleen het *lezen* van de status-/instellingenpagina blijft mogelijk zonder wachtwoord, met een zichtbare waarschuwing - zodat een apparaat waarvan de installatie nog niet is afgerond niet volledig ontoegankelijk is zonder seriële toegang.

4. Veilige configuratie — wat de gebruiker zelf moet doen

ACTIE	WAAROM
Stel bij de eerste installatie een wachtwoord in voor de instellingenpagina (verplicht veld)	Zonder wachtwoord is de instellingenpagina voor iedereen op hetzelfde wifi-netwerk te <i>lezen</i> (zonder inloggen); wijzigen wordt door het apparaat zelf geweigerd totdat dit is gedaan
Gebruik een uniek, sterk wifi-wachtwoord op het eigen thuisnetwerk	Het tijdelijke installatienetwerk van het apparaat zelf is bewust open (zie hieronder), maar dat is alleen actief tijdens de korte installatieperiode
Maak het apparaat niet vanaf buiten het thuisnetwerk bereikbaar (geen portforwarding)	De instellingenpagina is ontworpen voor gebruik binnen een vertrouwd netwerk
Houd het apparaat aangesloten op stroom, zodat automatische beveiligingsupdates ontvangen kunnen worden	Zie punt 6

Zie [hoofdstuk 5.2 van de Gebruikershandleiding](#) voor de installatiestappen, en [hoofdstuk 11 \(Privacy en beveiliging\)](#) voor meer achtergrond.

5. Beveiligingskenmerken van dit product

- **Versleutelde verbindingen:** alle verbindingen van het apparaat naar internet (ophalen van het afvalschema, software-updates) zijn TLS-versleuteld met certificaatvalidatie.
- **Geen wachtwoorden in platte tekst:** het wachtwoord van de instellingenpagina wordt gezouten en gehasht opgeslagen, nooit leesbaar.
- **Verplicht instellingenwachtwoord:** nieuwe apparaten vragen tijdens de eerste installatie een wachtwoord af (verplicht veld); het apparaat weigert elke instellingenwijziging totdat dit is gebeurd. Alleen lezen blijft mogelijk zonder wachtwoord, met een zichtbare waarschuwing.
- **Beveiligde software-updates:** firmware-updates worden opgehaald via een beveiligde verbinding. **Het apparaat verifieert de cryptografische handtekening van elke update (Secure Boot V2) en accepteert geen onjuist ondertekende of niet-ondertekende firmware.**

- **Lokale instellingenpagina:** bereikbaar op het eigen thuisnetwerk via gewone HTTP (geen TLS-terminatie op het apparaat zelf) - zie de toelichting in punt 3 over waarom het apparaat niet buiten het thuisnetwerk bereikbaar gemaakt moet worden.
- **Fabrieksreset:** alle opgeslagen gegevens (adres, wifi-gegevens, inloggegevens) kunnen op elk moment door de gebruiker gewist worden via de resetknop - zie hoofdstuk 9.5 van de Gebruikershandleiding.

6. Software-updates

Het apparaat controleert automatisch en periodiek (standaard elke 12 uur, instelbaar) of er een nieuwe firmwareversie beschikbaar is, en installeert deze zelfstandig - hier is geen actie van de gebruiker voor nodig, zolang het apparaat op stroom en verbonden met wifi blijft. De gebruiker kan dit ook handmatig direct laten controleren via de instellingenpagina.

7. Ondersteuningsperiode

Eagle Software Consultancy B.V. levert beveiligingsupdates voor dit productmodel (Garbi Sein v1) gedurende **minimaal 5 jaar** vanaf de datum waarop dit model voor het laatst nieuw is verkocht.

Eerste marktintroductie	17-september-2026
Verwachte einddatum van beveiligingsondersteuning	1-januari-2033

Deze datum wordt bijgewerkt zodra deze vaststaat, en uiterlijk 6 maanden vóór het einde van de ondersteuningsperiode opnieuw gepubliceerd met een duidelijke aankondiging op www.eaglesc.nl.

8. Kwetsbaarheden melden

Zie het [Coordinated Vulnerability Disclosure-beleid](#) - meldingen zijn welkom via security@eaglesc.nl.

Laatst bijgewerkt: 2026-09-17.