

# Beleid voor het melden van kwetsbaarheden (Coordinated Vulnerability Disclosure)

**Eagle Software Consultancy B.V. — geldt voor alle producten van het merk Garbi Sein.**

Wij stellen het op prijs als beveiligingsonderzoekers en gebruikers ons helpen onze producten veiliger te maken door kwetsbaarheden verantwoord bij ons te melden. Dit document beschrijft hoe u dat kunt doen, wat u van ons kunt verwachten, en binnen welke termijnen.

Dit beleid is opgesteld in lijn met de meldingsverplichtingen uit de EU Cyber Resilience Act (Verordening (EU) 2024/2847), Bijlage I, Deel II.

---

## Waar kunt u een kwetsbaarheid melden?

**E-mail:** [security@eaglesc.nl](mailto:security@eaglesc.nl)

Gebruik bij voorkeur deze route in plaats van ons algemene contactadres of sociale media, zodat uw melding direct bij de juiste persoon terechtkomt.

Voor een Garbi Sein-apparaat dat aangesloten en bereikbaar is, kan een probleem ook rechtstreeks vanaf het apparaat zelf gemeld worden via de knop **"Report a problem"** op de statuspagina ( `/status` ) - dit stuurt automatisch het apparaat-ID en de recente logregels mee. Voor een **beveiligingskwetsbaarheid** (in tegenstelling tot een functioneel probleem) heeft een melding via [security@eaglesc.nl](mailto:security@eaglesc.nl) de voorkeur, zodat deze niet tussen gewone probleemmeldingen verdwijnt.

---

## Wat te vermelden in uw melding

Om de melding snel te kunnen beoordelen, vragen we u waar mogelijk het volgende te vermelden:

- Een beschrijving van de kwetsbaarheid en de mogelijke impact.
  - Stappen om het probleem te reproduceren (proof-of-concept, indien van toepassing).
  - Het betrokken product, firmwareversie (te vinden op de statuspagina van het apparaat) en, indien relevant, het apparaat-ID.
  - Uw contactgegevens, zodat we bij vragen kunnen terugkoppelen (u mag anoniem melden, maar dan kunnen we u niet op de hoogte houden van de voortgang).
- 

## Wat u van ons kunt verwachten

| STAP                                                                       | TERMIJN                                                                       |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Ontvangstbevestiging                                                       | Binnen 3 werkdagen                                                            |
| Eerste inhoudelijke beoordeling (is het reproduceerbaar, wat is de impact) | Binnen 10 werkdagen                                                           |
| Statusupdate, ook als het onderzoek nog loopt                              | Ten minste elke 30 dagen                                                      |
| Oplossing (patch/mitigatie) of onderbouwde uitleg waarom niet              | Zo snel als redelijkerwijs mogelijk, afhankelijk van de complexiteit en ernst |

Voor kwetsbaarheden die **actief worden misbruikt** of die een **ernstig beveiligingsincident** vormen, hanteren wij de wettelijke meldtermijnen aan ENISA/CSIRT (vroegge waarschuwing binnen 24 uur, volledige melding binnen 72 uur, eindrapport binnen 14 dagen na kennisname) - een melding van u kan dit traject in gang zetten.

---

## Gecoördineerde openbaarmaking

We vragen u een gemelde kwetsbaarheid niet openbaar te maken (blog, sociale media, een CVE aanvragen zonder overleg, etc.) totdat:

- er een oplossing beschikbaar is en gebruikers redelijkerwijs de kans hebben gehad deze te installeren, of
- er **90 dagen** zijn verstreken sinds uw eerste melding zonder dat wij hebben gereageerd of een duidelijk tijdpad hebben gegeven,

**welke van beide zich het eerst voordoet.** We overleggen graag met u over een gezamenlijke publicatiedatum en vermelden, als u dat wilt, uw naam als melder bij de bekendmaking.

---

## Wat wij beloven

- We ondernemen geen juridische stappen tegen onderzoekers die deze procedure te goeder trouw volgen: geen toegang zoeken tot gegevens van andere gebruikers, geen verstoring van de dienstverlening veroorzaken, en ons de kans geven het probleem te verhelpen voordat het openbaar wordt gemaakt.
- We houden u op de hoogte van de voortgang, binnen de hierboven genoemde termijnen.
- Beveiligingsupdates worden kosteloos beschikbaar gesteld gedurende de ondersteuningsperiode van het product - zie [Product-Security-Support-Information](#).

---

## Reikwijdte

Dit beleid geldt voor:

- De firmware van Garbi Sein-apparaten.

- De backend-diensten die deze apparaten aanspreken op `eaglesc.nl` (bijvoorbeeld de firmware-update-check en de probleemmeldfunctie).

Dit beleid geldt **niet** voor kwetsbaarheden in diensten van derde partijen die het apparaat uitleest (afvalinzamelaars' eigen API's) - meld dergelijke problemen rechtstreeks bij de betreffende organisatie.

---

*Laatst bijgewerkt: 2026-09-12.*