

Cybersecurity-risicobeoordeling — publieke samenvatting

Garbi Sein v1 — Eagle Software Consultancy B.V.

Conform de EU Cyber Resilience Act (Verordening (EU) 2024/2847) voert Eagle Software Consultancy B.V. een cybersecurity-risicobeoordeling uit over de gehele levenscyclus van dit product, en houdt deze actueel bij elke significante wijziging aan het product. Dit document is een publieksvriendelijke samenvatting daarvan. Het volledige, gedetailleerde document wordt intern bewaard als onderdeel van het technisch documentatiedossier, en is desgevraagd beschikbaar voor toezichthoudende autoriteiten.

We publiceren bewust een samenvatting in plaats van het volledige detail: specifieke technische afwegingen over de precieze werking van beveiligingsmaatregelen zijn nuttiger voor een aanvaller dan voor een gebruiker, terwijl de conclusies en de genomen maatregelen dat niet zijn.

Aanpak

De beoordeling kijkt naar het product over de hele levenscyclus - ontwerp, productie, gebruik bij de klant thuis, software-updates, en einde van de ondersteuningsperiode - en naar de categorieën risico die relevant zijn voor een wifi-verbonden consumentenapparaat zonder beveiligings-kritische functie:

1. **Netwerkblootstelling:** welke poorten/diensten zijn bereikbaar, vanaf waar, en met welke authenticatie.
2. **Gegevensverwerking:** welke gegevens het apparaat verzamelt, verzendt en opslaat, en hoe deze beschermd worden.
3. **Software-updatemechanisme:** hoe wordt voorkomen dat het apparaat een niet-geautoriseerde firmware installeert.
4. **Fysieke/lokale toegang:** wat een aanvaller met fysieke toegang tot het apparaat zou kunnen, en welke mitigaties daartegen bestaan.
5. **Afhankelijkheid van externe diensten:** de risico's van het gebruik van API's van derde partijen (afvalinzamelaars) buiten de eigen controle van de fabrikant.

Belangrijkste conclusies

- Het apparaat heeft **geen** beveiligings-, toegangscontrole- of veiligheidskritische functie; een compromittering van het apparaat geeft geen toegang tot andere systemen in huis anders dan wat toegang tot het eigen wifi-netwerk sowieso al zou geven.

- Verbindingen naar internet zijn versleuteld en gevalideerd (TLS); er wordt geen ongevalideerde ("insecure") verbinding gebruikt.
- Wachtwoorden worden nooit in leesbare vorm opgeslagen.
- Firmware-updates worden **cryptografisch ondertekend gecontroleerd** vóór installatie (Secure Boot V2); het apparaat accepteert geen onjuist ondertekende firmware.
- De eerste installatie van het apparaat gebeurt via een tijdelijk, kortdurend eigen wifi-netwerk zonder wachtwoord - een bewuste, gedocumenteerde afweging (zie [Product-Security-Support-Information](#), punt 3) die standaard is voor consumentenapparaten van dit type en zonder seriële toegang voor de klant niet praktisch anders op te lossen is zonder een aanvullende fysieke provisioneringsstap (bijvoorbeeld een uniek label per apparaat) - dit wordt overwogen voor een toekomstige hardware-revisie.
- Een instellingenpagina-wachtwoord is verplicht: nieuwe apparaten vragen het tijdens de eerste installatie af (verplicht veld), en het apparaat weigert elke wijziging van de instellingen zolang er geen wachtwoord is ingesteld - met als enige uitzondering het instellen van dat eerste wachtwoord zelf. Voor reeds uitgerolde apparaten (van vóór deze maatregel) geldt dit vanaf het eerstvolgende moment dat de gebruiker iets wil wijzigen. Alleen het *lezen* van de status-/instellingenpagina blijft toegankelijk zonder wachtwoord, met een zichtbare waarschuwing, zodat een apparaat vóór het instellen van dat eerste wachtwoord niet volledig ontoegankelijk is.
- Het apparaat is afhankelijk van diverse externe, niet door de fabrikant beheerde API's van afvalinzamelaars voor zijn kernfunctie. Uitval of wijziging van zo'n API leidt in het slechtste geval tot een verouderd of ontbrekend ophaalschema, niet tot een beveiligingsrisico voor de gebruiker - het apparaat behoudt het laatst bekende schema totdat een nieuwe, succesvolle ophaling lukt.

Restrisico's die bewust geaccepteerd zijn

- Het ontbreken van een wachtwoord op het tijdelijke installatienetwerk tijdens de (kortdurende) installatiestap zelf (zie hierboven). Op de instellingenpagina is dit restrisico beperkt tot alleen leestoegang, en alleen totdat het (verplichte) eerste wachtwoord is ingesteld. Op dit moment heeft het apparaat ook nog geen toegang tot het wifi netwerk van de gebruiker, en kan derhalve geen negatieve effecten hebben.
- De instellingenpagina is bereikbaar via gewoon HTTP op het eigen thuisnetwerk (geen TLS-terminatie op het apparaat zelf) - acceptabel voor gebruik binnen een vertrouwd thuisnetwerk, maar reden om het apparaat nadrukkelijk niet vanaf buiten dat netwerk bereikbaar te maken (zie [Product-Security-Support-Information](#), punt 3).

Beide punten worden bij elke nieuwe productrevisie opnieuw beoordeeld.

Kwetsbaarheden melden

Zie het [Coordinated Vulnerability Disclosure-beleid](#).

Laatst bijgewerkt: 2026-09-17.