Beleid voor het melden van kwetsbaarheden

1. Doel

EGO Europe GmbH (hierna "de Organisatie") zet zich in voor het ontvangen, beoordelen en behandelen van meldingen van cyberbeveiligingskwetsbaarheden met betrekking tot haar producten met digitale elementen. Dit beleid beschrijft ons gecoördineerde proces voor het melden van kwetsbaarheden en ondersteunt onze naleving van de toepasselijke vereisten van Verordening (EU) 2024/2847 (de "EU Cyberweerbaarheidsverordening" of "CRA").

Wij zetten ons in om onze producten voortdurend te verbeteren, met aandacht voor veranderende marktbehoeften, opkomende dreigingen en nieuwe aanvalsvectoren.

2. Toepassingsgebied

U kunt een mogelijke cyberbeveiligingskwetsbaarheid melden die tijdens het gebruik van de volgende producten is aangetroffen:

- Applicaties (APP) en producten die met APP's kunnen verbinden
- Producten met diagnose-interfaces en de bijbehorende op afstand bestuurbare diagnosetools

3. Hoe een kwetsbaarheid te melden

3.1 Meldkanaal

Stuur ons geen informatie over een probleem via onbeveiligde kanalen. Meldingen van kwetsbaarheden dienen in plaats daarvan te worden ingediend via onze **e-mail**:

Beveiligingscontact: psirt@egopowerplus.eu

Als uw melding exploitcode, toegangsgegevens, persoonsgegevens of andere gevoelige informatie bevat, neem dan eerst contact met ons op, zodat wij een geschikte veilige overdrachtsmethode kunnen aanbieden.

Dit contactpunt wordt gecontroleerd door gekwalificeerd personeel en is niet beperkt tot geautomatiseerde tools.

3.2 Inhoud van de melding

Melders dienen, voor zover mogelijk, de volgende informatie te verstrekken voor een efficiënte triage:

- **Getroffen product of app**: exacte naam en versie, firmware- of softwareversie (essentieel)
- **Beschrijving van de kwetsbaarheid**: een gedetailleerde beschrijving van de kwetsbaarheid en de mogelijke gevolgen ervan
- **Stappen om te reproduceren**: stapsgewijze instructies, inclusief tools en omgevingsdetails
- **Ondersteunend bewijs**: schermafbeeldingen, netwerkopnames, logbestanden of proof-of-concept (PoC) code
- **Beoordeling van de ernst**: aanbevolen CVSS v3.1- of v4.0-score
- **Contactgegevens**: e-mailadres of andere contactgegevens voor verdere communicatie (essentieel)

3.3 Richtlijnen voor beveiligingsonderzoek

Bij het uitvoeren van beveiligingsonderzoek of tests vragen wij u:

- geen toegang te krijgen tot, te kopiëren, te wijzigen of te verwijderen van gegevens van andere gebruikers;
- geen gebruik te maken van social engineering, phishing, denial-of-service-aanvallen, fysieke aanvallen of andere methoden die onze producten, diensten of gebruikers kunnen verstoren;
- testen te beperken tot wat redelijkerwijs noodzakelijk is om de kwetsbaarheid te bevestigen en te documenteren;
- te stoppen met testen en ons onmiddellijk te informeren als u toegang krijgt tot persoonsgegevens, inloggegevens, vertrouwelijke informatie of systemen buiten het beoogde toepassingsgebied; en
- de kwetsbaarheid niet openbaar te maken voordat wij een redelijke gelegenheid hebben gehad om deze te onderzoeken en te verhelpen, behoudens toepasselijk recht.

Dit beleid geeft geen toestemming voor onwettig gedrag of gedrag dat de aan u verleende toegangsrechten overschrijdt.

4. Proces voor de afhandeling van kwetsbaarheden

Het Product Security Incident Response Team (PSIRT) zal na ontvangst van een melding van een kwetsbaarheid de kwetsbaarheidsbeoordeling en risico-evaluatie

uitvoeren. Bevestigde kwetsbaarheden worden verholpen en openbaar gemaakt, waarbij de noodzakelijke communicatie met de melder wordt onderhouden. Als wordt bevestigd dat de kwetsbaarheid zich in een upstreamcomponent bevindt, stelt PSIRT de leverancier op de hoogte.

Voorafgaand aan enige openbaarmaking dienen beide partijen overeenstemming te bereiken over het volgende:

- Datum van openbaarmaking
- Inhoud van een openbare aankondiging of verklaring
- Vereiste embargoperiode ter bescherming van gebruikers

5. Vertrouwelijkheid

De Organisatie zal meldingen van kwetsbaarheden vertrouwelijk behandelen en de persoonsgegevens van de melder niet zonder uitdrukkelijke toestemming aan derden verstrekken, tenzij wettelijk verplicht.

Melders kunnen ook anoniem blijven; anonimiteit kan echter het vermogen van de Organisatie om verdere communicatie te bieden beperken.

6. Erkenning

{ Organisatie / Persoon }

7. Verholpen kwetsbaarheden

Kwetsbaarheids-ID / Kwetsbaarheid	Impact	Getroffen product(en)	Ernst	Aanbevelingen
Geen verholpen kwetsbaarheden geregistreerd				