Politik for offentliggørelse af sårbarheder

1. Formål

EGO Europe GmbH (herefter "Organisationen") forpligter sig til at modtage, vurdere og håndtere rapporter om cybersikkerhedssårbarheder vedrørende sine produkter med digitale elementer. Denne politik beskriver vores koordinerede proces for offentliggørelse af sårbarheder og understøtter vores overholdelse af de gældende krav i forordning (EU) 2024/2847 ("EU's Cyber Resilience Act" eller "CRA").

Vi er engagerede i løbende at forbedre vores produkter med fokus på ændrede markedskrav, håndtering af nye trusler og tilpasning til nye angrebsvektorer.

2. Anvendelsesområde

Du kan rapportere en potentiel cybersikkerhedssårbarhed, som er konstateret ved brug af følgende produkter:

- Applikationer (APP) og produkter, der kan forbindes til APP'er
- Produkter med diagnoseinterfaces og tilhørende fjernstyrbare diagnoseværktøjer

3. Sådan rapporterer du en sårbarhed

3.1 Indberetningskanal

Send venligst ikke oplysninger om et problem til os via usikre kanaler. Rapporter om sårbarheder bør i stedet indsendes via vores **e-mail**:

Product Security Incident Response Team Contact: psirt@egopowerplus.eu;

Hvis din rapport indeholder exploit-kode, adgangsoplysninger, personoplysninger eller andre følsomme oplysninger, bedes du kontakte os først, så vi kan tilbyde en passende sikker overførselsmetode.

Dette kontaktpunkt overvåges af kvalificeret personale og er ikke begrænset til automatiserede værktøjer.

3.2 Rapportens indhold

Indberettere bør i videst muligt omfang oplyse følgende for at muliggøre effektiv prioritering:

- **Berørt produkt eller app**: nøjagtigt navn og version, firmware- eller softwareversion (obligatorisk)
- **Beskrivelse af sårbarheden**: en detaljeret beskrivelse af sårbarheden og dens potentielle konsekvenser
- **Trin til at genskabe fejlen**: trinvise instruktioner, herunder værktøjer og miljødetaljer
- **Understøttende dokumentation**: skærmbilleder, netværksoptagelser, logfiler eller proof of concept-kode (PoC)
- **Vurdering af alvorlighed**: anbefalet CVSS v3.1- eller v4.0-score
- **Kontaktoplysninger**: e-mail eller andre kontaktoplysninger til opfølgning (obligatorisk)

3.3 Retningslinjer for sikkerhedsforskning

Når du udfører sikkerhedsforskning eller test, bedes du:

- undgå at tilgå, kopiere, ændre eller slette data, der tilhører andre brugere;
- undlade at anvende social engineering, phishing, denial-of-service-angreb, fysiske angreb eller andre metoder, der kan forstyrre vores produkter, tjenester eller brugere;
- begrænse testen til, hvad der med rimelighed er nødvendigt for at bekræfte og dokumentere sårbarheden;
- stoppe testen og straks underrette os, hvis du får adgang til personoplysninger, adgangsoplysninger, fortrolige oplysninger eller systemer uden for det tilsigtede omfang; og
- undlade offentligt at afsløre sårbarheden, før vi har haft en rimelig mulighed for at undersøge og afhjælpe den, med forbehold for gældende lovgivning.

Denne politik giver ikke tilladelse til ulovlig adfærd eller adfærd, der går ud over de adgangstilladelser, du er givet.

4. Proces for håndtering af sårbarheder

Product Security Incident Response Team (PSIRT) vil foretage sårbarhedsvurdering og risikovurdering ved modtagelse af en sårbarhedsrapport. Bekræftede sårbarheder vil blive afhjulpet og offentliggjort, med den nødvendige kommunikation opretholdt

med indberetteren. Hvis sårbarheden bekræftes at ligge i en opstrømskomponent, vil PSIRT underrette leverandøren.

Forud for enhver offentliggørelse bør begge parter nå til enighed om følgende:

- Dato for offentliggørelse
- Indhold af enhver offentlig meddelelse eller erklæring
- Nødvendig karensperiode for at beskytte brugerne

5. Fortrolighed

Organisationen vil behandle rapporter om sårbarheder fortroligt og vil ikke dele indberetterens personoplysninger med tredjeparter uden udtrykkeligt samtykke, medmindre det kræves ved lov.

Indberettere kan også forblive anonyme; anonymitet kan dog begrænse Organisationens mulighed for at give opfølgende kommunikation.

6. Anerkendelse

{ Organisation / Person }

7. Afhjulpne og offentliggjorte sårbarheder

Sårbarheds-ID/sårbarhed	Konsekvens	Berørt(e) produkt(er)	Alvorlighed	Anbefalinger
Ingen afhjulpne sårbarheder registreret				