

# Haavoittuvuuksien julkistamiskäytäntö

## 1. Tarkoitus

**EGO Europe GmbH** (jäljempänä "Organisaatio") sitoutuu vastaanottamaan, arvioimaan ja käsittelemään digitaalisia elementtejä sisältäviin tuotteisiinsa liittyviä kyberturvallisuuden haavoittuvuusraportteja. Tämä käytäntö kuvaa koordinoitua haavoittuvuuksien julkistamisprosessiamme ja tukee vaatimustenmukaisuuttamme asetuksen (EU) 2024/2847 ("EU:n kyberkestävyysäädös" tai "CRA") sovellettavien vaatimusten kanssa.

Olemme sitoutuneet parantamaan tuotteitamme jatkuvasti keskittyen muuttuviin markkinatarpeisiin, uusiin uhkiin vastaamiseen ja uusiin hyökkäysvektoreihin sopeutumiseen.

## 2. Soveltamisala

Voit ilmoittaa mahdollisesta kyberturvallisuuden haavoittuvuudesta, joka on havaittu seuraavien tuotteiden käytön aikana:

- Sovellukset (APP) ja tuotteet, jotka voivat muodostaa yhteyden sovelluksiin
- Diagnostiikkarajapinnoilla varustetut tuotteet ja niihin liittyvät etäohjattavat diagnostiikkatyökalut

## 3. Näin ilmoitat haavoittuvuudesta

### 3.1 Ilmoituskanava

Älä lähetä meille tietoja ongelmasta suojaamattomien kanavien kautta. Sen sijaan haavoittuvuusraportit tulee toimittaa **sähköpostitse**:

**Turvallisuusyhteyshetimit:** [psirt@egopowerplus.eu](mailto:psirt@egopowerplus.eu)

Jos raporttisi sisältää hyväksikäyttökoodia, käyttöoikeustietoja, henkilötietoja tai muita arkaluonteisia tietoja, ota ensin yhteyttä meihin, jotta voimme tarjota sopivan turvallisen siirtomenetelmän.

Tätä yhteyspistettä valvoo pätevä henkilöstö, eikä se rajoitu pelkästään automatisoituihin työkaluihin.

## 3.2 Raportin sisältö

Ilmoittajien tulisi mahdollisuuksien mukaan antaa seuraavat tiedot tehokkaan priorisoinnin mahdollistamiseksi:

- **Vaikutuksen kohteena oleva tuote tai sovellus:** Tarkka nimi ja versio, laiteohjelmiston tai ohjelmiston versio (välttämätön)
- **Haavoittuvuuden kuvaus:** yksityiskohtainen kuvaus haavoittuvuudesta ja sen mahdollisista vaikutuksista
- **Toistovaiheet:** vaiheittaiset ohjeet, mukaan lukien työkalut ja ympäristön tiedot
- **Tukevat todisteet:** kuvakaappaukset, verkkotallenteet, lokit tai konseptin toimivuuden todistava (PoC) koodi
- **Vakavuuden arviointi:** suositeltu CVSS v3.1- tai v4.0-pistemäärä
- **Yhteystiedot:** sähköposti tai muut yhteystiedot jatkaviestintää varten (välttämätön)

## 3.3 Tietoturvatutkimuksen ohjeet

Kun teet tietoturvatutkimusta tai testausta, pyydämme sinua:

- välttämään muiden käyttäjien tietoihin pääsyä, niiden kopioimista, muuttamista tai poistamista;
- olemaan käyttämättä social engineering -menetelmiä, tietojenkalastelua, palvelunestohyökkäyksiä, fyysisiä hyökkäyksiä tai muita menetelmiä, jotka voivat häiritä tuotteitamme, palveluitamme tai käyttäjiämme;
- rajoittamaan testauksen siihen, mikä on kohtuudella tarpeen haavoittuvuuden vahvistamiseksi ja dokumentoimiseksi;
- lopettamaan testauksen ja ilmoittamaan meille välittömästi, jos pääset käsiksi henkilötietoihin, tunnistetietoihin, luottamuksellisiin tietoihin tai järjestelmiin suunnitellun laajuuden ulkopuolella; ja
- olemaan julkistamatta haavoittuvuutta ennen kuin meillä on ollut kohtuullinen mahdollisuus tutkia ja korjata se, sovellettavan lainsäädännön mukaisesti.

Tämä käytäntö ei oikeuta laittomaan toimintaan tai toimintaan, joka ylittää sinulle myönnettyt käyttöoikeudet.

## 4. Haavoittuvuuksien käsittelyprosessi

Tuoteturvallisuuden häiriötilanteisiin reagoiva tiimi (PSIRT) suorittaa haavoittuvuuden ja riskin arvioinnin saatuaan haavoittuvuusraportin. Vahvistetut haavoittuvuudet korjataan ja julkistetaan, ja tarvittavaa viestintää ilmoittajan kanssa ylläpidetään. Jos

haavoittuvuuden vahvistetaan sijaitsevan alkupään komponentissa, PSIRT ilmoittaa toimittajalle.

Ennen mahdollista julkistamista molempien osapuolten tulisi sopia seuraavista:

- Julkistamispäivä
- Mahdollisen julkisen ilmoituksen tai lausunnon sisältö
- Käyttäjien suojaamiseksi vaadittava karenssi aika

5. Luottamuksellisuus

Organisaatio pitää haavoittuvuusraportit luottamuksellisina eikä jaa ilmoittajan henkilötietoja kolmansille osapuolille ilman nimenomaista suostumusta, ellei laki sitä edellytä.

Ilmoittajat voivat myös pysyä nimettöminä; nimettömyys voi kuitenkin rajoittaa Organisaation kykyä tarjota jatkaviestintää.

6. Kiitokset

{ Organisaatio / Henkilö }

7. Korjatut ja julkistetut haavoittuvuudet

| Haavoittuvuustunnus / Haavoittuvuus           | Vaikutus | Vaikutuksen kohteena oleva(t) tuote(et) | Vakavuus | Suositukset |
|-----------------------------------------------|----------|-----------------------------------------|----------|-------------|
| Ei rekisteröityjä korjattuja haavoittuvuuksia |          |                                         |          |             |