# Pažeidžiamumų atskleidimo politika

## 1. Tikslas

**„EGO Europe GmbH“** (toliau – „Organizacija“) įsipareigoja priimti, vertinti ir spręsti kibernetinio saugumo pažeidžiamumų, susijusių su jos skaitmeninių elementų turinčiais gaminiais, pranešimus. Ši politika apibūdina mūsų koordinuotą pažeidžiamumų atskleidimo procesą ir padeda užtikrinti atitiktį taikomiems Reglamento (ES) 2024/2847 ("ES Kibernetinio atsparumo aktas" arba "CRA") reikalavimams.

Esame įsipareigoję nuolat tobulinti savo gaminius, atsižvelgdami į kintančius rinkos poreikius, spręsdami kylančias grėsmes ir prisitaikydami prie naujų atakų vektorių.

## 2. Taikymo sritis

Galite pranešti apie galimą kibernetinio saugumo pažeidžiamumą, aptiktą naudojant šiuos gaminius:

- Programėles (APP) ir gaminius, kurie gali prisijungti prie programėlių
- Gaminius su diagnostikos sąsajomis ir su jais susijusius nuotoliniu būdu valdomus diagnostikos įrankius

## 3. Kaip pranešti apie pažeidžiamumą

### 3.1 Pranešimo kanalas

Prašome nesiųsti mums informacijos apie problemą nesaugiais kanalais. Vietoj to, pranešimai apie pažeidžiamumus turėtų būti teikiami mūsų **el. paštu**:

Saugumo kontaktas: psirt@egopowerplus.eu

Jei jūsų pranešime yra išnaudojimo kodas, prieigos duomenys, asmens duomenys ar kita jautri informacija, prašome pirmiausia susisiekti su mumis, kad galėtume pasiūlyti tinkamą saugų perdavimo būdą.

Šį kontaktinį punktą stebi kvalifikuoti darbuotojai, o jis neapsiriboja automatizuotomis priemonėmis.

### 3.2 Pranešimo turinys
Pranešėjai, kiek įmanoma, turėtų pateikti šią informaciją, kad būtų galima efektyviai prioritetizuoti:

- **Paveiktas gaminys ar programėlė**: tikslus pavadinimas ir versija, aparatinės ar programinės įrangos versija (būtina)
- **Pažeidžiamumo aprašymas**: išsamus pažeidžiamumo ir jo galimo poveikio aprašymas
- **Atkūrimo veiksmai**: nuoseklios instrukcijos, įskaitant įrankius ir aplinkos duomenis
- **Patvirtinantys įrodymai**: ekrano nuotraukos, tinklo srauto įrašai, žurnalai arba koncepcijos įrodymo (PoC) kodas
- **Sunkumo vertinimas**: rekomenduojamas CVSS v3.1 arba v4.0 balas
- **Kontaktinė informacija**: el. paštas ar kiti kontaktiniai duomenys tolesniam bendravimui (būtina)

### 3.3 Saugumo tyrimų gairės
Atlikdami saugumo tyrimus ar testavimą, prašome:

- nesinaudoti, nekopijuoti, nekeisti ir netrinti kitų vartotojų duomenų;
- nenaudoti socialinės inžinerijos, sukčiavimo apsimetant (phishing), paslaugų trikdymo atakų, fizinių atakų ar kitų metodų, galinčių sutrikdyti mūsų gaminius, paslaugas ar vartotojus;
- apriboti testavimą tiek, kiek pagrįstai būtina pažeidžiamumui patvirtinti ir dokumentuoti;
- nutraukti testavimą ir nedelsiant mus informuoti, jei gaunate prieigą prie asmens duomenų, prisijungimo duomenų, konfidencialios informacijos ar sistemų, nepatenkančių į numatytą apimtį; ir
- viešai neatskleisti pažeidžiamumo, kol neturėjome pagrįstos galimybės jį ištirti ir pašalinti, laikantis taikomų teisės aktų.

Ši politika nesuteikia teisės atlikti neteisėtų veiksmų arba veiksmų, viršijančių jums suteiktus prieigos leidimus.

## 4. Pažeidžiamumų valdymo procesas
Gaminių saugumo incidentų reagavimo komanda (PSIRT), gavusi pranešimą apie pažeidžiamumą, atliks pažeidžiamumo ir rizikos vertinimą. Patvirtinti pažeidžiamumai bus pašalinti ir atskleisti, palaikant reikalingą ryšį su pranešėju. Jei patvirtinama, kad pažeidžiamumas yra pirminiame (upstream) komponente, PSIRT informuos tiekėją.

Prieš bet kokį viešą atskleidimą abi šalys turėtų susitarti dėl:

- Atskleidimo datos
- Bet kokio viešo pranešimo ar pareiškimo turinio
- Reikiamo moratoriumo laikotarpio vartotojams apsaugoti

## 5. Konfidencialumas

Organizacija saugos pranešimus apie pažeidžiamumus konfidencialiai ir nesidalins pranešėjo asmens duomenimis su trečiosiomis šalimis be aiškaus sutikimo, išskyrus atvejus, kai to reikalauja įstatymai.

Pranešėjai taip pat gali likti anonimiški; tačiau anonimiškumas gali riboti Organizacijos galimybes teikti tolesnį bendravimą.

## 6. Padėka

**{ Organizacija / Asmuo }**

## 7. Pašalinti ir atskleisti pažeidžiamumai

| Pažeidžiamumo ID / pažeidžiamumas | Poveikis | Paveiktas (-i) gaminys (-iai) | Sunkumas | Rekomendacijos |
|---|---|---|---|---|
| *Pašalintų pažeidžiamumų nėra užregistruota* | | | | |