Turvanõrkustest teatamise põhimõtted

1. Eesmärk

EGO Europe GmbH (edaspidi "Organisatsioon") on pühendunud oma digielemente sisaldavate toodete küberturvalisuse nõrkustest teatamiste vastuvõtmisele, hindamisele ja käsitlemisele. Käesolev põhimõte kirjeldab meie koordineeritud nõrkustest teatamise protsessi ning toetab vastavust määruse (EL) 2024/2847 ("ELi küberturvalisuse akt" ehk "CRA") kohaldatavatele nõuetele.

Oleme pühendunud oma toodete pidevale täiustamisele, keskendudes muutuvatele turunõuetele, uutele ohtudele ja uutele ründevektoritele kohanemisele.

2. Kohaldamisala

Võimalikust küberturvalisuse nõrkusest, mis on avastatud järgmiste toodete kasutamisel, võite teatada:

- Rakendused (APP) ja tooted, mis saavad ühenduda rakendustega
- Diagnostikaliidestega tooted ja nendega seotud kaugjuhitavad diagnostikavahendid

3. Kuidas teatada nõrkusest

3.1 Teatamiskanal

Palun ärge saatke meile probleemi puudutavat teavet ebaturvaliste kanalite kaudu. Selle asemel tuleks nõrkusest teatada meie **e-posti** teel:

Turvakontakt: psirt@egopowerplus.eu

Kui teie teade sisaldab rünnet võimaldavat koodi, juurdepääsuandmeid, isikuandmeid või muud tundlikku teavet, võtke meiega palun esmalt ühendust, et saaksime pakkuda sobivat turvalist edastusviisi.

Seda kontaktpunkti jälgib kvalifitseeritud personal ja see ei piirdu automatiseeritud vahenditega.

3.2 Teate sisu

Teatajad peaksid võimaluste piires esitama tõhusaks prioriseerimiseks järgmise teabe:

- **Mõjutatud toode või rakendus**: täpne nimi ja versioon, püsivara või tarkvara versioon (kohustuslik)
- **Nõrkuse kirjeldus**: üksikasjalik kirjeldus nõrkusest ja selle võimalikust mõjust
- **Taasesitamise sammud**: samm-sammulised juhised, sealhulgas vahendid ja keskkonna üksikasjad
- **Toetavad tõendid**: ekraanitõmmised, võrguandmete jäädvustused, logid või kontseptsiooni tõestuse (PoC) kood
- **Tõsiduse hindamine**: soovitatav CVSS v3.1 või v4.0 skoor
- **Kontaktandmed**: e-post või muud kontaktandmed järelsuhtluseks (kohustuslik)

3.3 Turvauuringute juhised

Turvauuringute või testimise läbiviimisel palume teil:

- vältida teiste kasutajate andmetele juurdepääsu, nende kopeerimist, muutmist või kustutamist;
- mitte kasutada sotsiaalmanipulatsiooni, andmepüüki, teenusetõkestusründeid, füüsilisi ründeid ega muid meetodeid, mis võivad häirida meie tooteid, teenuseid või kasutajaid;
- piirduda testimisel sellega, mis on mõistlikult vajalik nõrkuse kinnitamiseks ja dokumenteerimiseks;
- peatada testimine ja teavitada meid viivitamata, kui pääsete ligi isikuandmetele, mandaatidele, konfidentsiaalsele teabele või süsteemidele, mis jäävad ette nähtud ulatusest väljapoole; ning
- mitte avaldada nõrkust avalikult enne, kui meil on olnud mõistlik võimalus seda uurida ja kõrvaldada, kohaldatava õiguse piires.

Käesolev põhimõte ei anna luba ebaseaduslikuks tegevuseks ega tegevuseks, mis ületab teile antud juurdepääsuõigusi.

4. Nõrkuste käsitlemise protsess

Toote turvaintsidentidele reageerimise meeskond (PSIRT) viib pärast nõrkusest teatamise saamist läbi nõrkuse ja riski hindamise. Kinnitatud nõrkused kõrvaldatakse ja avalikustatakse, säilitades vajaliku suhtluse teatajaga. Kui kinnitatakse, et nõrkus asub ülesvoolu komponendis, teavitab PSIRT tarnijat.

Enne avalikustamist peaksid mõlemad pooled jõudma kokkuleppele järgmises:

- Avalikustamise kuupäev

- Avaliku teate või avalduse sisu
- Kasutajate kaitsmiseks vajalik embargoperiood

5. Konfidentsiaalsus

Organisatsioon hoiab nõrkusest teatamised konfidentsiaalsena ega jaga teataja isikuandmeid kolmandate isikutega ilma selgesõnalise nõusolekuta, välja arvatud juhul, kui seadus seda nõuab.

Teatajad võivad jääda ka anonüümseks; anonüümsus võib siiski piirata Organisatsiooni võimet pakkuda järelsuhtlust.

6. Tunnustus

{ Organisatsioon / Isik }

7. Kõrvaldatud ja avalikustatud nõrkused

Nõrkuse ID / nõrkus	Mõju	Mõjutatud toode(tooted)	Tõsidus	Soovitused
Registreeritud kõrvaldatud nõrkusi ei ole				