Sebezhetőségek Nyilvánosságra Hozatali Szabályzata

1. Cél

Az EGO Europe GmbH (a továbbiakban: "a Szervezet") elkötelezett amellett, hogy fogadja, értékelje és kezelje a digitális elemeket tartalmazó termékeivel kapcsolatos kiberbiztonsági sebezhetőségi jelentéseket. Jelen szabályzat ismerteti a koordinált sebezhetőség-nyilvánosságra hozatali folyamatunkat, és támogatja a(z) (EU) 2024/2847 rendelet (az "EU Kiberrezilencia-jogszabály" vagy "CRA") vonatkozó követelményeinek való megfelelésünket.

Elkötelezettek vagyunk termékeink folyamatos fejlesztése iránt, a változó piaci igényekre összpontosítva, kezelve a felmerülő fenyegetéseket, és alkalmazkodva az új támadási vektorokhoz.

2. Hatály

A következő termékek használata során észlelt esetleges kiberbiztonsági sebezhetőséget jelentheti:

- Alkalmazások (APP) és az alkalmazásokhoz csatlakozni képes termékek
- Diagnosztikai interfésszel rendelkező termékek és a hozzájuk kapcsolódó, távolról vezérelhető diagnosztikai eszközök

3. Hogyan jelentsen sebezhetőséget

3.1 Bejelentési csatorna

Kérjük, ne küldjön nekünk információt egy problémáról nem biztonságos csatornákon keresztül. Ehelyett a sebezhetőségi jelentéseket **e-mailben** kell benyújtani:

Biztonsági kapcsolattartó: psirt@egopowerplus.eu

Ha jelentése kihasználó (exploit) kódot, hozzáférési adatokat, személyes adatokat vagy más érzékeny információt tartalmaz, kérjük, először vegye fel velünk a kapcsolatot, hogy megfelelő, biztonságos átviteli módszert biztosíthassunk.

Ezt a kapcsolattartási pontot képzett személyzet felügyeli, és nem korlátozódik automatizált eszközökre.

3.2 A jelentés tartalma

A bejelentőknek a lehető legnagyobb mértékben az alábbi információkat kell megadniuk a hatékony rangsorolás érdekében:

- **Érintett termék vagy alkalmazás**: Pontos név és verzió, firmware- vagy szoftververzió (alapvető)
- **A sebezhetőség leírása**: a sebezhetőség és lehetséges hatásának részletes leírása
- **A reprodukálás lépései**: lépésről lépésre útmutató, beleértve az eszközöket és a környezeti adatokat
- **Alátámasztó bizonyítékok**: képernyőképek, hálózati rögzítések, naplók vagy koncepcióigazoló (PoC) kód
- **Súlyossági értékelés**: ajánlott CVSS v3.1 vagy v4.0 pontszám
- **Elérhetőségi adatok**: e-mail vagy egyéb elérhetőségi adatok a további kommunikációhoz (alapvető)

3.3 Biztonsági kutatási irányelvek

Biztonsági kutatás vagy tesztelés végzésekor kérjük, hogy:

- kerülje más felhasználók adataihoz való hozzáférést, azok másolását, módosítását vagy törlését;
- ne alkalmazzon social engineeringet, adathalászatot, szolgáltatásmegtagadási támadásokat, fizikai támadásokat vagy más olyan módszereket, amelyek zavarhatják termékeinket, szolgáltatásainkat vagy felhasználóinkat;
- a tesztelést korlátozza arra, ami ésszerűen szükséges a sebezhetőség megerősítéséhez és dokumentálásához;
- állítsa le a tesztelést, és azonnal értesítsen minket, ha személyes adatokhoz, hitelesítő adatokhoz, bizalmas információkhoz vagy a tervezett hatókörön kívül eső rendszerekhez fér hozzá; és
- ne hozza nyilvánosságra a sebezhetőséget, mielőtt ésszerű lehetőségünk lett volna kivizsgálni és orvosolni azt, a vonatkozó jogszabályok figyelembevételével.

Jelen szabályzat nem jogosít fel jogellenes magatartásra, illetve a Önnek biztosított hozzáférési engedélyeket meghaladó magatartásra.

4. Sebezhetőségkezelési folyamat

A Termékbiztonsági Incidensreagáló Csapat (PSIRT) a sebezhetőségi jelentés kézhezvételét követően elvégzi a sebezhetőség és a kockázat értékelését. A megerősített sebezhetőségeket orvosolják és nyilvánosságra hozzák, a bejelentővel fenntartott szükséges kommunikáció mellett. Ha megerősítést nyer, hogy a sebezhetőség egy upstream összetevőben található, a PSIRT értesíti a beszállítót.

Bármilyen nyilvánosságra hozatal előtt mindkét félnek meg kell állapodnia a következőkről:

- A nyilvánosságra hozatal dátuma
- Bármilyen nyilvános közlemény vagy nyilatkozat tartalma
- A felhasználók védelméhez szükséges embargó időszak

5. Titoktartás

A Szervezet bizalmasan kezeli a sebezhetőségi jelentéseket, és nem osztja meg a bejelentő személyes adatait harmadik felekkel kifejezett hozzájárulás nélkül, kivéve, ha ezt jogszabály előírja.

A bejelentők névtelenek is maradhatnak; a névtelenség azonban korlátozhatja a Szervezet azon képességét, hogy további kommunikációt biztosítson.

6. Elismerés

{ Szervezet / Magánszemély }

7. Orvosolt és nyilvánosságra hozott sebezhetőségek

Sebezhetőség azonosítója / Sebezhetőség	Hatás	Érintett termék(ek)	Súlyosság	Ajánlások
Nincs nyilvántartott, orvosolt sebezhetőség				