Richtlinie zur Offenlegung von Schwachstellen

1. Zweck

EGO Europe GmbH (im Folgenden "die Organisation") verpflichtet sich, Berichte über Cybersicherheitsschwachstellen in Bezug auf ihre Produkte mit digitalen Elementen entgegenzunehmen, zu bewerten und zu bearbeiten. Diese Richtlinie beschreibt unseren koordinierten Prozess zur Offenlegung von Schwachstellen und unterstützt die Einhaltung der geltenden Anforderungen der Verordnung (EU) 2024/2847 (der "EU Cyber Resilience Act" oder "CRA").

Wir setzen uns dafür ein, unsere Produkte kontinuierlich zu verbessern, indem wir uns auf sich wandelnde Marktanforderungen einstellen, neu auftretenden Bedrohungen begegnen und uns an neue Angriffsvektoren anpassen.

2. Geltungsbereich

Sie können eine potenzielle Cybersicherheitsschwachstelle melden, die bei der Nutzung der folgenden Produkte festgestellt wurde:

- Anwendungen (APP) und Produkte, die eine Verbindung zu APPs herstellen können
- Produkte mit Diagnoseschnittstellen und den zugehörigen fernsteuerbaren Diagnosewerkzeugen

3. Wie Sie eine Schwachstelle melden

3.1 Meldekanal

Bitte senden Sie uns keine Informationen zu einem Problem über unsichere Kanäle. Stattdessen sollten Schwachstellenberichte über unsere **E-Mail** eingereicht werden:

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

Wenn Ihr Bericht Exploit-Code, Zugangsdaten, personenbezogene Daten oder andere sensible Informationen enthält, kontaktieren Sie uns bitte zunächst, damit wir eine geeignete sichere Übertragungsmethode bereitstellen können.

Diese Kontaktstelle wird von qualifiziertem Personal überwacht und ist nicht auf automatisierte Werkzeuge beschränkt.

3.2 Inhalt der Meldung

Meldende Personen sollten, soweit möglich, folgende Informationen bereitstellen, um eine effiziente Triage zu ermöglichen:

- **Betroffenes Produkt oder App**: Genauer Name und Version, Firmware- oder Softwareversion (erforderlich)
- **Beschreibung der Schwachstelle**: eine detaillierte Beschreibung der Schwachstelle und ihrer potenziellen Auswirkungen
- **Schritte zur Reproduktion**: schrittweise Anleitung, einschließlich Werkzeuge und Umgebungsdetails
- **Unterstützende Nachweise**: Screenshots, Netzwerkmitschnitte, Protokolle oder Proof-of-Concept-Code (PoC)
- **Bewertung des Schweregrads**: empfohlener CVSS-Wert v3.1 oder v4.0
- **Kontaktinformationen**: E-Mail-Adresse oder andere Kontaktdaten für die Nachverfolgung (erforderlich)

3.3 Leitlinien für Sicherheitsforschung

Bei der Durchführung von Sicherheitsforschung oder -tests bitten wir Sie:

- nicht auf Daten anderer Nutzer zuzugreifen, diese zu kopieren, zu verändern oder zu löschen;
- kein Social Engineering, Phishing, Denial-of-Service-Angriffe, physische Angriffe oder andere Methoden anzuwenden, die unsere Produkte, Dienste oder Nutzer stören könnten;
- Tests auf das zur Bestätigung und Dokumentation der Schwachstelle angemessen erforderliche Maß zu beschränken;
- Tests einzustellen und uns umgehend zu benachrichtigen, falls Sie auf personenbezogene Daten, Zugangsdaten, vertrauliche Informationen oder Systeme außerhalb des vorgesehenen Umfangs zugreifen; und
- die Schwachstelle nicht öffentlich offenzulegen, bevor wir eine angemessene Gelegenheit hatten, sie zu untersuchen und zu beheben, vorbehaltlich geltenden Rechts.

Diese Richtlinie berechtigt nicht zu rechtswidrigem Verhalten oder zu einem Verhalten, das über die Ihnen gewährten Zugriffsberechtigungen hinausgeht.

4. Prozess zur Bearbeitung von Schwachstellen

Das Product Security Incident Response Team (PSIRT) führt nach Eingang eines Schwachstellenberichts die Schwachstellenbewertung und Risikoeinschätzung durch. Bestätigte Schwachstellen werden behoben und offengelegt, wobei die erforderliche Kommunikation mit der meldenden Person aufrechterhalten wird. Wird bestätigt, dass sich die Schwachstelle in einer vorgelagerten Komponente befindet, benachrichtigt das PSIRT den Zulieferer.

Vor jeder öffentlichen Offenlegung sollten sich beide Parteien auf Folgendes einigen:

- Offenlegungsdatum
- Inhalt einer öffentlichen Ankündigung oder Erklärung
- Erforderliche Sperrfrist zum Schutz der Nutzer

5. Vertraulichkeit

Die Organisation behandelt Schwachstellenberichte vertraulich und gibt die persönlichen Daten der meldenden Person ohne deren ausdrückliche Zustimmung nicht an Dritte weiter, es sei denn, dies ist gesetzlich vorgeschrieben.

Meldende Personen können auch anonym bleiben; Anonymität kann jedoch die Fähigkeit der Organisation einschränken, eine Nachverfolgung zu ermöglichen.

6. Anerkennung

{ Organisation / Einzelperson }

7. Behobene Schwachstellenoffenlegungen

Schwachstellen-ID / Schwachstelle	Auswirkung	Betroffene(s) Produkt(e)	Schweregrad	Empfehlungen
Keine behobenen Schwachstellen verzeichnet				