Politica di divulgazione delle vulnerabilità

1. Finalità

EGO Europe GmbH (di seguito "l'Organizzazione") si impegna a ricevere, valutare e affrontare le segnalazioni di vulnerabilità di cybersicurezza relative ai propri prodotti con elementi digitali. La presente Politica descrive il nostro processo coordinato di divulgazione delle vulnerabilità e sostiene la conformità ai requisiti applicabili del Regolamento (UE) 2024/2847 (il "Cyber Resilience Act dell'UE" o "CRA").

Ci impegniamo a migliorare continuamente i nostri prodotti, tenendo conto dell'evoluzione delle esigenze di mercato, affrontando le minacce emergenti e adattandoci a nuovi vettori di attacco.

2. Ambito di applicazione

È possibile segnalare una potenziale vulnerabilità di cybersicurezza riscontrata durante l'uso dei seguenti prodotti:

- Applicazioni (APP) e prodotti che possono connettersi ad APP
- Prodotti con interfacce diagnostiche e i relativi strumenti diagnostici controllabili da remoto

3. Come segnalare una vulnerabilità

3.1 Canale di segnalazione

Si prega di non inviarci informazioni relative a un problema tramite canali non sicuri. Le segnalazioni di vulnerabilità devono invece essere inviate tramite la nostra **email**:

Contatto di sicurezza: psirt@egopowerplus.eu

Se la segnalazione contiene codice di exploit, credenziali di accesso, dati personali o altre informazioni sensibili, vi preghiamo di contattarci preventivamente affinché possiamo fornire un metodo di trasferimento sicuro adeguato.

Questo punto di contatto è monitorato da personale qualificato e non si limita a strumenti automatizzati.

3.2 Contenuto della segnalazione

I segnalanti dovrebbero fornire, per quanto possibile, le seguenti informazioni per una gestione efficiente della priorità:

- **Prodotto o App interessato/a**: nome esatto e versione, versione del firmware o del software (essenziale)
- **Descrizione della vulnerabilità**: una descrizione dettagliata della vulnerabilità e del suo potenziale impatto
- **Passaggi per la riproduzione**: istruzioni passo dopo passo, compresi strumenti e dettagli sull'ambiente
- **Prove a supporto**: screenshot, acquisizioni di rete, log o codice Proof of Concept (PoC)
- **Valutazione della gravità**: punteggio CVSS v3.1 o v4.0 consigliato
- **Informazioni di contatto**: indirizzo email o altri recapiti per il seguito della comunicazione (essenziale)

3.3 Linee guida per la ricerca sulla sicurezza

Durante l'esecuzione di ricerche o test di sicurezza, si prega di:

- evitare di accedere, copiare, alterare o eliminare dati appartenenti ad altri utenti;
- non utilizzare ingegneria sociale, phishing, attacchi denial-of-service, attacchi fisici o altri metodi che possano interrompere i nostri prodotti, servizi o utenti;
- limitare i test a quanto ragionevolmente necessario per confermare e documentare la vulnerabilità;
- interrompere i test e comunicarcelo tempestivamente qualora si acceda a dati personali, credenziali, informazioni riservate o sistemi al di fuori dell'ambito previsto; e
- non divulgare pubblicamente la vulnerabilità prima che abbiamo avuto una ragionevole opportunità di analizzarla e porvi rimedio, fatta salva la legge applicabile.

La presente Politica non autorizza condotte illecite né condotte che eccedano le autorizzazioni di accesso concesse.

4. Processo di gestione delle vulnerabilità

Il Product Security Incident Response Team (PSIRT) effettuerà la valutazione della vulnerabilità e dei rischi al ricevimento di una segnalazione. Le vulnerabilità confermate saranno risolte e divulgate, mantenendo la necessaria comunicazione

con il segnalante. Se si conferma che la vulnerabilità risiede in un componente a monte, il PSIRT informerà il fornitore.

Prima di qualsiasi divulgazione pubblica, entrambe le parti dovrebbero raggiungere un accordo su quanto segue:

- Data di divulgazione
- Contenuto di eventuali comunicati o dichiarazioni pubbliche
- Periodo di embargo necessario per proteggere gli utenti

5. Riservatezza

L'Organizzazione manterrà riservate le segnalazioni di vulnerabilità e non condividerà i dati personali del segnalante con terzi senza consenso esplicito, salvo quanto richiesto dalla legge.

I segnalanti possono anche rimanere anonimi; tuttavia, l'anonimato può limitare la capacità dell'Organizzazione di fornire un seguito alla comunicazione.

6. Riconoscimento

{ Organizzazione / Persona }

7. Vulnerabilità risolte e divulgate

ID vulnerabilità / Vulnerabilità	Impatto	Prodotto/i interessato /i	Gravità	Raccomandazioni
Nessuna vulnerabilità risolta registrata				