Politique de divulgation des vulnérabilités

1. Objet

EGO Europe GmbH (ci-après dénommée "l'Organisation") s'engage à recevoir, évaluer et traiter les signalements de vulnérabilités de cybersécurité concernant ses produits comportant des éléments numériques. La présente politique décrit notre processus coordonné de divulgation des vulnérabilités et appuie notre conformité aux exigences applicables du règlement (UE) 2024/2847 (le "règlement européen sur la cyber-résilience" ou "CRA").

Nous nous engageons à améliorer continuellement nos produits, en tenant compte de l'évolution des demandes du marché, en répondant aux menaces émergentes et en nous adaptant aux nouveaux vecteurs d'attaque.

2. Champ d'application

Vous pouvez signaler une vulnérabilité de cybersécurité potentielle constatée dans les produits suivants lors de leur utilisation :

- Applications (APP) et produits pouvant se connecter à des APP
- Produits dotés d'interfaces de diagnostic et outils de diagnostic contrôlables à distance associés

3. Comment signaler une vulnérabilité

3.1 Canal de soumission

Merci de ne pas nous transmettre d'informations sur un problème via des canaux non sécurisés. Les signalements de vulnérabilités doivent plutôt être soumis via notre **e-mail** :

Contact sécurité : psirt@egopowerplus.eu

Si votre signalement contient du code d'exploitation, des identifiants d'accès, des données personnelles ou d'autres informations sensibles, veuillez nous contacter au préalable afin que nous puissions vous fournir une méthode de transfert sécurisée appropriée.

Ce point de contact est surveillé par du personnel qualifié et ne se limite pas à des outils automatisés.

3.2 Contenu du signalement

Les personnes signalantes doivent fournir, dans la mesure du possible, les informations suivantes afin de faciliter un tri efficace :

- **Produit ou application concerné(e)** : nom exact et version, version du micrologiciel ou du logiciel (essentiel)
- **Description de la vulnérabilité** : une description détaillée de la vulnérabilité et de son impact potentiel
- **Étapes de reproduction** : instructions étape par étape, y compris les outils et les détails de l'environnement
- **Éléments justificatifs** : captures d'écran, captures réseau, journaux ou code de démonstration (PoC)
- **Évaluation de la gravité** : score CVSS v3.1 ou v4.0 recommandé
- **Coordonnées de contact** : adresse e-mail ou autres coordonnées pour un suivi (essentiel)

3.3 Lignes directrices pour la recherche en sécurité

Lors de la conduite de recherches ou de tests de sécurité, veuillez :

- éviter d'accéder aux données d'autres utilisateurs, de les copier, de les modifier ou de les supprimer ;
- ne pas recourir à l'ingénierie sociale, au hameçonnage, aux attaques par déni de service, aux attaques physiques ou à d'autres méthodes susceptibles de perturber nos produits, services ou utilisateurs ;
- limiter les tests à ce qui est raisonnablement nécessaire pour confirmer et documenter la vulnérabilité ;
- cesser les tests et nous en informer rapidement si vous accédez à des données personnelles, des identifiants, des informations confidentielles ou des systèmes en dehors du périmètre prévu ; et
- ne pas divulguer publiquement la vulnérabilité avant que nous ayons eu une possibilité raisonnable de l'examiner et d'y remédier, sous réserve du droit applicable.

La présente politique n'autorise aucune conduite illégale ni n'excède les autorisations d'accès qui vous sont accordées.

4. Processus de traitement des vulnérabilités

L'équipe de réponse aux incidents de sécurité produit (PSIRT) procédera à l'évaluation de la vulnérabilité et des risques dès réception d'un signalement. Les vulnérabilités confirmées seront corrigées et divulguées, une communication nécessaire étant maintenue avec la personne signalante. Si la vulnérabilité est confirmée comme résidant dans un composant en amont, le PSIRT en informera le fournisseur.

Avant toute divulgation publique, les deux parties devront se mettre d'accord sur les éléments suivants :

- Date de divulgation
- Contenu de toute annonce ou déclaration publique
- Période d'embargo requise pour protéger les utilisateurs

5. Confidentialité

L'Organisation conservera les signalements de vulnérabilités de manière confidentielle et ne partagera pas les informations personnelles de la personne signalante avec des tiers sans son consentement explicite, sauf si la loi l'exige.

Les personnes signalantes peuvent également rester anonymes ; toutefois, l'anonymat peut limiter la capacité de l'Organisation à assurer un suivi.

6. Remerciements

{ Organisation / Particulier }

7. Vulnérabilités corrigées et divulguées

Identifiant de vulnérabilité / Vulnérabilité	Impact	Produit(s) concerné(s)	Gravité	Recommandations
Aucune vulnérabilité corrigée enregistrée à ce jour				