Política de divulgación de vulnerabilidades

1. Objeto

EGO Europe GmbH (en adelante, "la Organización") se compromete a recibir, evaluar y abordar los informes de vulnerabilidades de ciberseguridad relativos a sus productos con elementos digitales. Esta Política describe nuestro proceso coordinado de divulgación de vulnerabilidades y respalda el cumplimiento de los requisitos aplicables del Reglamento (UE) 2024/2847 (la "Ley de Ciberresiliencia de la UE" o "CRA").

Estamos comprometidos con la mejora continua de nuestros productos, atendiendo a la evolución de las demandas del mercado, haciendo frente a las amenazas emergentes y adaptándonos a nuevos vectores de ataque.

2. Ámbito de aplicación

Puede notificar una posible vulnerabilidad de ciberseguridad detectada durante el uso de los siguientes productos:

- Aplicaciones (APP) y productos que puedan conectarse a APP
- Productos con interfaces de diagnóstico y sus herramientas de diagnóstico controlables de forma remota asociadas

3. Cómo notificar una vulnerabilidad

3.1 Canal de notificación

Le rogamos que no nos envíe información sobre ningún problema a través de canales no seguros. Los informes de vulnerabilidades deben enviarse a través de nuestro **correo electrónico**:

Contacto de seguridad: psirt@egopowerplus.eu

Si su informe contiene código de explotación, credenciales de acceso, datos personales u otra información sensible, póngase en contacto con nosotros primero para que podamos proporcionarle un método de transferencia seguro adecuado.

Este punto de contacto está supervisado por personal cualificado y no se limita a herramientas automatizadas.

3.2 Contenido del informe

Los notificantes deben proporcionar, en la medida de lo posible, la siguiente información para facilitar una clasificación eficiente:

- **Producto o aplicación afectada**: nombre y versión exactos, versión de firmware o software (esencial)
- **Descripción de la vulnerabilidad**: una descripción detallada de la vulnerabilidad y su posible impacto
- **Pasos para reproducirla**: instrucciones paso a paso, incluidas herramientas y detalles del entorno
- **Pruebas justificativas**: capturas de pantalla, capturas de red, registros o código de prueba de concepto (PoC)
- **Evaluación de la gravedad**: puntuación CVSS v3.1 o v4.0 recomendada
- **Información de contacto**: correo electrónico u otros datos de contacto para el seguimiento (esencial)

3.3 Directrices para la investigación en seguridad

Al realizar investigaciones o pruebas de seguridad, le rogamos que:

- evite acceder, copiar, alterar o eliminar datos pertenecientes a otros usuarios;
- no utilice ingeniería social, phishing, ataques de denegación de servicio, ataques físicos u otros métodos que puedan alterar nuestros productos, servicios o usuarios;
- limite las pruebas a lo razonablemente necesario para confirmar y documentar la vulnerabilidad;
- detenga las pruebas y nos notifique de inmediato si accede a datos personales, credenciales, información confidencial o sistemas fuera del alcance previsto; y
- no divulgue públicamente la vulnerabilidad antes de que hayamos tenido una oportunidad razonable de investigarla y solucionarla, sujeto a la legislación aplicable.

Esta Política no autoriza conductas ilícitas ni que excedan los permisos de acceso que se le hayan concedido.

4. Proceso de gestión de vulnerabilidades

El Equipo de Respuesta a Incidentes de Seguridad de Productos (PSIRT) llevará a cabo la evaluación de la vulnerabilidad y del riesgo tras la recepción de un informe. Las vulnerabilidades verificadas serán corregidas y divulgadas, manteniendo la comunicación necesaria con el notificante. Si se confirma que la vulnerabilidad reside en un componente ascendente, el PSIRT lo notificará al proveedor.

Antes de cualquier divulgación pública, ambas partes deberán llegar a un acuerdo sobre lo siguiente:

- Fecha de divulgación
- Contenido de cualquier anuncio o declaración pública
- Período de embargo necesario para proteger a los usuarios

5. Confidencialidad

La Organización mantendrá la confidencialidad de los informes de vulnerabilidades y no compartirá la información personal del notificante con terceros sin su consentimiento explícito, salvo que la ley lo exija.

Los notificantes también pueden permanecer en el anonimato; sin embargo, el anonimato puede limitar la capacidad de la Organización para proporcionar comunicación de seguimiento.

6. Reconocimiento

{ Organización / Persona }

7. Vulnerabilidades corregidas y divulgadas

ID de vulnerabilidad / Vulnerabilidad	Impacto	Producto(s) afectado(s)	Gravedad	Recomendaciones
No hay vulnerabilidades corregidas registradas				