POLÍTICA DE DIVULGACIÓN COORDINADA DE VULNERABILIDADES

ÍNDICE

INTRODUCCIÓN Y COMPROMISO

En BeePlanet Factory S.L. consideramos que la colaboración con la comunidad de seguridad, clientes y cualquier persona que detecte una vulnerabilidad es fundamental para mantener la seguridad de nuestros productos y servicios.

Esta política describe cómo se puede reportar una vulnerabilidad de seguridad detectada en nuestros productos, qué puede esperarse de nuestra parte durante el proceso, y en qué condiciones actuamos ante dichos reportes.

Nos comprometemos a investigar de buena fe todo reporte recibido conforme a esta política, a mantener informada a la persona que lo remite durante el proceso, y a corregir las vulnerabilidades confirmadas dentro de un plazo razonable.

ALCANCE

Esta política aplica a los productos y servicios digitales comercializados por BeePlanet Factory S.L.

Quedan fuera de esta política:

- Vulnerabilidades en infraestructura, sistemas o servicios de terceros no operados directamente por BeePlanet.
- Ataques de denegación de servicio (DoS/DDoS) o pruebas que puedan degradar la disponibilidad del servicio.
- Técnicas de ingeniería social dirigidas a empleados, clientes o proveedores.
- Acceso físico no autorizado a instalaciones o dispositivos.

Cualquier prueba de seguridad debe limitarse a lo estrictamente necesario para demostrar la existencia de la vulnerabilidad, evitando en todo momento el acceso, modificación o extracción de datos que no sean propios de quien reporta.

CÓMO REPORTAR

Para reportar una vulnerabilidad detectada en nuestros productos o servicios, puede rellenarse el formulario disponible desde la web o mandar un correo electrónico a la dirección seguridad@beeplanetfactory.com

Para agilizar el análisis, se solicita incluir en el reporte, en la medida de lo posible:

- Producto y versión afectados.
- Descripción técnica de la vulnerabilidad identificada.
- Pasos para reproducirla o prueba de concepto (PoC), si está disponible.
- Impacto potencial que se ha identificado.
- Datos de contacto para el seguimiento (pueden mantenerse anónimos si así se prefiere, aunque esto puede limitar nuestra capacidad de dar seguimiento al reporte).

Si el hallazgo es especialmente sensible, se recomienda cifrar la comunicación.

QUÉ PUEDE ESPERAR LA PERSONA QUE REPORTA

Una vez recibido un reporte a través del canal indicado, BeePlanet se compromete a:

- Confirmar la recepción del reporte en un plazo máximo de 72 horas.
- Realizar una evaluación inicial y comunicar si el reporte ha sido validado como una vulnerabilidad, en un plazo estimado de (pendiente de fijar).
- Mantener informada a la persona que reporta sobre el progreso durante el proceso de corrección, con actualizaciones periódicas si el proceso se extiende en el tiempo.
- Notificar cuando la vulnerabilidad haya sido corregida.

Estos plazos son orientativos y pueden variar según la complejidad técnica de la vulnerabilidad reportada.

REGLAS DE BUENA CONDUCTA

BeePlanet se compromete a no emprender acciones legales contra cualquier persona que reporte una vulnerabilidad de buena fe y conforme a esta política.

Este compromiso está condicionado a que la persona que reporta:

- Actúe con el único propósito de identificar y comunicar la vulnerabilidad, sin intención maliciosa.
- Evite el acceso, modificación, eliminación o extracción de datos que no le pertenezcan, más allá de lo estrictamente necesario para demostrar la vulnerabilidad.
- No divulgue públicamente la vulnerabilidad antes del plazo de embargo acordado.
- Actúe de forma proporcionada, evitando cualquier acción que pueda degradar la disponibilidad o integridad de los sistemas afectados.
- Respete el alcance definido.

El incumplimiento de estas condiciones puede dejar sin efecto el compromiso de no emprender acciones legales.

EMBARGO Y DIVULGACIÓN COORDINADA

BeePlanet solicita a la persona que reporta una vulnerabilidad que no la divulgue públicamente hasta que se haya publicado la corrección correspondiente o hasta que se cumpla el plazo de embargo acordado, lo que ocurra antes.

Como referencia general, el plazo de embargo estándar es de 90 días desde la recepción del reporte, pudiendo ampliarse si la complejidad de la corrección lo requiere, previa comunicación a la persona que reporta.

La fecha final de divulgación pública se acuerda conjuntamente entre BeePlanet y la persona que reporta, buscando en todo momento equilibrar la necesidad de informar a los usuarios con el tiempo necesario para aplicar la corrección de forma segura.

RECONOCIMIENTO

BeePlanet valora la contribución de quienes reportan vulnerabilidades de forma responsable. Por defecto, la identidad de la persona que reporta se mantiene confidencial y no se publica ni se comunica a terceros.

No se ofrece reconocimiento público ni recompensa económica (programa de *bug bounty*) asociados a esta política.

EXCLUSIONES

No se consideran reportes válidos conforme a esta política:

- Hallazgos que no supongan una vulnerabilidad real de seguridad (ej. problemas de configuración específicos del entorno del cliente, no atribuibles al producto).
- Vulnerabilidades ya conocidas por BeePlanet y que se encuentren en proceso de corrección.
- Vulnerabilidades en componentes o dependencias de terceros no controlados directamente por BeePlanet (conforme al alcance material definido internamente).
- Reportes genéricos de buenas prácticas de seguridad sin evidencia de una vulnerabilidad explotable concreta.

BeePlanet se reserva el derecho de determinar, tras su análisis, si un reporte queda dentro o fuera del alcance de esta política.

CONTACTO

Para reportar una vulnerabilidad conforme a esta política, puede utilizarse el canal indicado en el apartado 3.

Polígono Industrial Ipertegui II, 12 Orkoien 31160 – Navarra – España

info@beeplanetfactory.com

+34 948 234 386

www.beeplanetfactory.com