SOLIDWARETOOLS

CRACheck

DOCUMENTO 6

Política de Divulgación Coordinada de Vulnerabilidades

Anexo I, Parte II, punto 5 + Art. 13.8

NovaBridge Technologies Inc.

NovaBridge SmartHub v3.1

Referencia: CRACHK-NYCRWG
Fecha de emisión: 15/10/2026
Contacto: Sarah Chen, VP of Compliance
compliance@novabridge.io

Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo
de 23 de octubre de 2024 (Cyber Resilience Act)

Este documento no constituye asesoramiento jurídico. Responsabilidad exclusiva del fabricante.

>> POLÍTICA DE DIVULGACIÓN COORDINADA DE VULNERABILIDADES

Conforme al Anexo I, Parte II, punto 5 del Reglamento (UE) 2024/2847, el fabricante debe establecer y aplicar una política de divulgación coordinada de vulnerabilidades (Coordinated Vulnerability Disclosure — CVD). Este documento establece el proceso estructurado para recibir, gestionar y divulgar vulnerabilidades.

1. Ámbito

Esta política aplica al producto NovaBridge SmartHub v3.1 y a todos los componentes software y hardware que lo integran, incluyendo la solución de remote data processing asociada (si aplica).

2. Canal de reporte

PUNTO DE CONTACTO [Art. 13.17]

security@novabridge.io · https://www.novabridge.io/security · +1 302 555 0142 (horario EST)

El fabricante permite a los investigadores elegir su medio de comunicación preferido. El punto de contacto no se basa exclusivamente en herramientas automatizadas (Art. 13.17).

3. Proceso de gestión

DESCRIPCIÓN

Política de divulgación coordinada publicada en https://www.novabridge.io/security/cvd-policy. Canal de reporte: security@novabridge.io + formulario web HTTPS. Compromiso de acuse de recibo en 48 horas laborables. Tiempo de remediación objetivo: 90 días desde la confirmación de la vulnerabilidad. Divulgación pública coordinada tras la disponibilidad del parche. Programa de bug bounty activo en HackerOne (https://hackerone.com/novabridge) con recompensas de $100-$5,000 según severidad CVSS.

4. Tiempos de respuesta

ACUSE DE RECIBO

Según el proceso de gestión (apartado 3)

EVALUACIÓN INICIAL

Según el proceso de gestión (apartado 3)

REMEDIACIÓN OBJETIVO

Según clasificación CVSS — ver proceso de remediación (Documento 3)

DIVULGACIÓN COORDINADA

Tras la disponibilidad del parche, coordinando con el investigador

5. Publicación de vulnerabilidades corregidas

Conforme al Anexo I, Parte II, punto 4, tras la disponibilidad de una actualización de seguridad, el fabricante publica: descripción de la vulnerabilidad, productos afectados, impacto, severidad e información clara para que los usuarios apliquen la corrección. En casos justificados, la publicación puede diferirse hasta que los usuarios hayan tenido oportunidad de aplicar el parche.

6. Protección del investigador

El fabricante no emprenderá acciones legales contra investigadores de seguridad que reporten vulnerabilidades de buena fe y de forma responsable, conforme a esta política.

Este documento no constituye asesoramiento jurídico. Responsabilidad exclusiva del fabricante.

Este documento ha sido generado por CRACheck (SolidwareTools) a partir de la información facilitada por el fabricante. No constituye asesoramiento jurídico ni una auditoría de terceros. La veracidad de los datos y el cumplimiento efectivo de las obligaciones legales aplicables son responsabilidad exclusiva del fabricante. La estructura sigue el Reglamento (UE) 2024/2847 según la revisión de SolidwareTools a la fecha de emisión. Para asesoramiento personalizado, consulte con un profesional cualificado.