Política de seguridad y de divulgación de vulnerabilidades

UnderStack es el fabricante de UnderStack Code a efectos del Reglamento de Ciberresiliencia de la UE (CRA). Agradecemos las notificaciones de vulnerabilidades y las gestionamos mediante divulgación coordinada.

Cómo notificar

Envíe un correo electrónico a **security@understack.dk** con:

- la versión de la aplicación (Settings › About & legal) y la versión de macOS;
- una descripción, los pasos para reproducirla y el impacto que haya observado;
- si desea que se le reconozca la autoría y con qué nombre.

Le rogamos que no incluya datos personales que no sean necesarios. Contacto legible por máquina: https://understack.dk/.well-known/security.txt

Nuestros compromisos

- Acuse de recibo en un plazo de 3 días hábiles y una evaluación en un plazo de 10 días hábiles.
- Información actualizada al menos cada 14 días hasta que se corrija el problema.
- Plazos objetivo de corrección: crítica, 7 días; alta, 30 días; media, 90 días; baja, en la siguiente versión ordinaria.
- Las actualizaciones de seguridad son gratuitas y se proporcionan para todas las versiones con soporte al menos hasta el 31 de diciembre de 2031.
- Un aviso público cuando la corrección esté disponible, reconociendo su autoría si así lo desea.
- Si una vulnerabilidad está siendo explotada activamente, la notificamos al CSIRT competente y a ENISA según exige el CRA, e informamos a los usuarios de la medida de mitigación que deben aplicar.

Puerto seguro

La investigación de buena fe que siga esta política es bienvenida y no emprenderemos acciones legales contra ella. Le rogamos que: realice pruebas únicamente en sistemas y datos de su propiedad; no acceda a datos de otras personas, ni los modifique ni los conserve, más allá de una prueba de concepto mínima; no degrade los servicios; no recurra a ingeniería social ni a ataques físicos; nos conceda un plazo razonable (hasta 90 días) para corregir el problema antes de su divulgación pública.

Fuera del alcance

La calidad de los resultados de los modelos de IA (las respuestas incorrectas no son vulnerabilidades, salvo que eludan el sistema de aprobaciones), los problemas que requieran una cuenta de macOS ya comprometida y las vulnerabilidades en servicios o modelos de terceros: notifíquelas a sus responsables de mantenimiento e infórmenos si la forma en que UnderStack Code los utiliza agrava el impacto.

Lista de materiales de software

Cada versión incluye una SBOM en formato CycloneDX y los avisos de licencias de terceros, visibles en Settings › About & legal.