

Security and Vulnerability Disclosure Policy

UnderStack is the manufacturer of UnderStack Code under the EU Cyber Resilience Act. We welcome reports of vulnerabilities and handle them under coordinated disclosure.

How to report

Email [**security@understack.dk**](mailto:security@understack.dk) with:

- the app version (Settings › About & legal) and macOS version;
- a description, steps to reproduce and the impact you observed;
- whether you want to be credited, and under which name.

Please do not include personal data that is not needed. Machine-readable contact: <https://understack.dk/.well-known/security.txt>

What we promise

- Acknowledgement within 3 working days, and an assessment within 10 working days.
- Updates at least every 14 days until the issue is fixed.
- Fix targets: critical 7 days, high 30 days, medium 90 days, low in the next regular release.
- Security updates are free of charge and provided for every supported version until at least 31 December 2031.
- A public advisory when the fix is available, crediting you if you wish.
- If a vulnerability is actively exploited, we report it to the competent CSIRT and ENISA as the CRA requires, and inform users with the mitigation to apply.

Safe harbour

Good-faith research that follows this policy is welcome, and we will not take legal action against it. Please: test only on systems and data you own; do not access, change or keep other people's data beyond a minimal proof of concept; do not degrade services; no social engineering or physical attacks; give us reasonable time (up to 90 days) to fix before public disclosure.

Out of scope

Quality of AI model output (incorrect answers are not vulnerabilities unless they bypass the approval system), issues that require an already compromised macOS account, and vulnerabilities in third-party services or models — report those to their maintainers, and tell us if the way UnderStack Code uses them makes the impact worse.

Software bill of materials

Each release includes a CycloneDX SBOM and the third-party licence notices, visible in Settings > About & legal.