

AN OSS SCAN THAT YOU CAN ACT ON

Prepare the project and decide who owns each finding.

Anthropic OSS Scanner is an opt-in service for eligible open-source projects. Core maintainers enroll through a configuration PR. Fast-track reports have not undergone human review and need maintainer validation.

Prepare for enrollment

1. Read eligibility criteria and confirm you are a core maintainer with capacity to triage findings.
2. Start from the official project template. Prepare the repository URL, primary contact and a Dockerfile that builds the audit environment.
3. Document the threat model: exposed inputs, important assets, areas in scope and how to reproduce a meaningful issue.
4. Run the repository's configuration validator and build the Dockerfile locally. Confirm the test suite works in that environment.

Triage the report

1. Reproduce the claimed behavior in a controlled test. Record the affected revision and prerequisites.
2. Separate confirmed vulnerabilities, duplicates and false positives. Assign an owner and add a regression test to the fix.
3. Use the project's disclosure process for confirmed issues. Keep unvalidated claims out of public incident statements.

Prepare these fields

Repository: _____
Maintainer/contact: _____
Build environment: _____
Threat model location: _____
Triage owner and review date: _____

ORIGINAL RESOURCE

[Anthropic OSS Scanner enrollment guide](https://red.anthropic.com/oss-scanner)

<https://red.anthropic.com/oss-scanner>

An independent companion by Huzaifa Shoukat. Check the original project for current setup and availability. Prepared 12 October 2026.