Security policy and bug bounty program

This page describes general best practices for reporting bugs and provides specific reporting guidelines for OP Stack and OP Mainnet code contained within theethereum-optimism(opens in a new tab) GitHub organization.

Do not disclose vulnerabilities publicly or by executing them against a production network. If you do, you will not only be putting users at risk, but you will forfeit your right to a reward. Always follow the appropriate reporting pathways as described below.

- Do not
- disclose the vulnerability publicly, for example by filing a public ticket.
- Do not
- test the vulnerability on a publicly available network, either the testnet or the mainnet.

Optimism bug bounty program

The Optimism Bug Bounty Program offers up to2,000,042(opens in a new tab) for critical vulnerabilities found in the OP Mainnet codebase. Below you can find information about the various available bug bounty programs and how to report bugs that are not covered by an existing bounty.

Main bounty page

Optimism has a very detailedBug Bounty Page on Immunefi(opens in a new tab). In the listing you can find all the information relating to components in scope, reporting, and the payout process.

Unscoped bugs

If you think you have found a significant bug or vulnerabilities in OP Stack smart contracts, infrastructure, etc., even if that component is not covered by an existing bug bounty, please report it via theImmunefi program(opens in a new tab). The impact of any and all reported issues will be considered and the program has previously rewarded security researchers for bugs not within its stated scope.

Reporting other vulnerabilities

For vulnerabilities in any websites, email servers, or other non-critical infrastructure within the OP Stack, please contact the Foundation's service provider at and include detailed instructions for confirming and reproducing the vulnerability.

Vulnerability disclosure

Each OP Stack component maintainer may determine its own process for vulnerability disclosure. However, the following describes a recommended process for disclosure.

In the event that an OP Stack component maintainer learns of a critical security vulnerability, the maintainer reserves the right to silently fix it without immediately publicly disclosing the existence or nature of the vulnerability.

In such a scenario, the disclosure process used is as follows:

1. Silently fix the vulnerability and include the fix in release X.
2. After 4-8 weeks, disclose that release X contained a security fix.
3. After an additional 4-8 weeks, publish details of the vulnerability, along with credit to the reporter (with express permission from the reporter).

Rights of maintainers

Alongside this policy, maintainers also reserve the right to:

- Bypass this policy and publish details on a shorter timeline.
- Directly notify a subset of downstream users prior to making a public announcement.

This policy is based on theGeth(opens in a new tab) team'ssilent patch policy(opens in a new tab).