Bug Bounty

Participate in the Safe Bug Bounty program to find bugs and get rewards. Earn up to $1,000,000 for every bug you report. Please carefully read through thesubmission process section and get in touch viabounty@safe.global . You can also review thebug bounties we have paid in the past.

Audits

Smart contract security experts have carefully audited Safe's contracts. Please refer to thesecurity audits page for details.

Rules

Many of theEthereum Foundation's bug bounty program rules(opens in a new tab) are also applicable to the Safe Bug Bounty program:

- Issues already submitted by another user or known to the Safe team aren't eligible for bounty rewards.
- Public disclosure of a vulnerability makes it ineligible for a bounty.
- The Safe core development team, employees, and all other people paid by Safe, directly or indirectly (including the external auditors), aren't eligible for rewards.
- The Safe Bounty program considers several variables in determining rewards. Determinations of eligibility, score, and all terms related to an award are at the sole and final discretion of the Safe Bug Bounty panel.

Scope

The scope of the bug bounty program includes the core contracts related to the following releases of the Safe contracts:

- v1.4.1 (Release details(opens in a new tab)
- ,README(opens in a new tab)
-)
- v1.3.0
- (Release details(opens in a new tab)
- ,README(opens in a new tab)
-)
- v1.2.0
- (Release details(opens in a new tab)
- ,README(opens in a new tab)
-)
- v1.1.1
- (Release details(opens in a new tab)
- ,README(opens in a new tab)
-)

The scope of the bug bounty also includes theAllowance Module(opens in a new tab) .

In scope

Safe core contracts (version 1.4.1)

- Safe.sol (formerly GnosisSafe.sol)
- SafeL2.sol (formerly GnosisSafeL2.sol)
- SafeProxyFactory.sol (formerly GnosisSafeProxyFactory.sol)
- SafeProxy.sol (formerly GnosisSafeProxy.sol)
- MultiSend.sol, MultiSendCallOnly.sol, CreateCall.sol
- TokenCallbackHandler.sol (formerly DefaultCallbackHandler.sol), CompatibilityFallbackHandler.sol, HandlerContext.sol

You can find addresses for deployed instances of these contractshere or in theSafe deployments(opens in a new tab) repository.

Gnosis Safe core contracts (up to version 1.3.0)

- GnosisSafe.sol
- GnosisSafeL2.sol
- GnosisSafeProxyFactory.sol (formerly ProxyFactory.sol)
- GnosisSafeProxy.sol (formerly Proxy.sol)
- CreateAndAddModules.sol, MultiSend.sol, MultiSendCallOnly.sol, CreateCall.sol
- DefaultCallbackHandler.sol, CompatibilityFallbackHandler.sol, HandlerContext.sol

You can find addresses for deployed instances of these contracts here in the Safe deployments (opens in a new tab) repository.

Safe Modules contracts

- AllowanceModule.sol

Examples of what's in scope

- Being able to steal funds
- Being able to freeze funds or render them inaccessible by their owners
- Being able to perform replay attacks on the same chain
- Being able to change Safe settings or module settings without the consent of owners

Out of scope

- Any files, Safe Modules, or libraries other than the ones mentioned above
- More efficient gas solutions
- Any points listed as an already known weaknesses
- Any points listed in the audit or formal verification results reports
- Any points fixed in a newer version

Intended behavior

Please refer to the README file (opens in a new tab) and the release details (opens in a new tab) of the respective contract version on GitHub as well as our developer docs (opens in a new tab) for an extensive overview of the intended behavior of the smart contracts.

For the allowance module, please refer to the corresponding README file (opens in a new tab).

Compensation

All bugs (they don't necessarily need to lead to a redeploy) will be considered for a bounty, but the severity of the threat will change the reward. Below are the reward levels for each threat severity and an example of such a threat.

High threat: Up to $1,000,000

An identified attack that could steal funds or tokens or lock user funds would be considered a high threat. Likewise, a reported bug that, on its own, leads to a redeploy of the code will always be regarded as a high threat.

Medium threat: Up to $50,000

An identified attack where it's possible to steal funds because of unexpected behavior on the user's part. Unexpected behavior here means the user can't anticipate and comprehend that they will lose the funds.

Low threat: Up to $10,000

A way to avoid transaction fees or an exploit that in some way compromises the experience of other Safe users.

Safe will pay all bounties in ETH.

Please note that the submission's quality will factor into the level of compensation. A high-quality submission should include an explanation of how somebody can reproduce the bug.

Submission Process

Please email your submissions to bounty@safe.global .

Remember to include your ETH address so that you may be rewarded. If more than one address is specified, Safe will use only one at the discretion of the bounty program administrators. Anonymous submissions are welcome, too.

Please consult our privacy policy (opens in a new tab) for further details on how we handle submissions.

Responsible Disclosure Policy

If you comply with the policies below when reporting a security issue to us, we won't initiate a lawsuit or law enforcement investigation against you in response to your report.

We ask that:

- You give us reasonable time to investigate and mitigate an issue you report before making public any information about the report or sharing such information with others.
- You make a good faith effort to avoid privacy violations and disruptions to others, including (but not limited to) data destruction and interruption or degradation of our services.
- You don't exploit a security issue you discover for any reason. This includes demonstrating additional risk, such as an attempted compromise of sensitive company data or probing for additional issues.
- You don't violate any other applicable laws or regulations.

Public disclosure of the bug or the indication of an intention to exploit it on Mainnet will make the report ineligible for a bounty. If in doubt about other aspects of the bounty, most of the Ethereum Foundation bug bounty program rules(opens in a new tab) will apply here.

Any questions? Reach us via email (bounty@safe.global) or Discord(opens in a new tab) . For more information on the Safe, check out our website(opens in a new tab) and our GitHub(opens in a new tab) .

Happy hunting!

Note on Safe{Wallet}

Generally, bugs and issues regarding Safe{Wallet} frontend or backend are out of scope . This refers to the web app(opens in a new tab) , mobile apps, as well as the wallet backend services. For general bug reports, please consider submitting an issue on the respective repository such as safe-wallet-web(opens in a new tab) .

Please only use bounty@safe.global for severe security-related issues. We will carefully check all submissions; however, rewards remain voluntarily at our sole discretion.

Audits Past Paid Bounties

Was this page helpful?

Report issue