Bug Bounty

Program Overview

This bug bounty is specifically for Drift's smart contract code; client / UI only bugs are omitted.

Drift's smart contract isopen-source(opens in a new tab) .

Severity Description Bug Bounty Critical Bugs that freeze user funds or drain the contract's holdings or involve the theft of funds without user signatures. 10% of the value of the hack up to 500,000. High Bugs that couldtemporarily freeze user funds or incorrectly assign value to user funds. 10,000 to 50,000 per bug, assessed on a case-by-case basis Medium/Low Bugs that don't threaten user funds 1,000 to 5,000 per bug, assessed on a case-by-case basis The severity guidelines are based onImmunefi's classification system(opens in a new tab) .

Note that these are simply guidelines for the severity of the bugs. Each bug bounty submission will be evaluated on a case-by-case basis.

Submission

Please emailhello@drift.trade with a detailed description of the attack vector. For critical and moderate bugs, we require a proof of concept done on a privately deployed mainnet contract. We will reach back out in 1 business day with additional questions or the next steps on the bug bounty.

Bug Bounty Payment

Bug bounties will be paid in USDC. Alternative payment methods can be used on a case-by-case basis.

Invalid Bug Bounties

The following are out of scope for the bug bounty:

- Attacks that the reporter has already exploited themselves, leading to damage
- Attacks requiring access to leaked keys/credentials
- Attacks requiring access to privileged addresses (governance, admin)
- Incorrect data supplied by third-party oracles (This does not exclude oracle manipulation/flash loan attacks)
- Lack of liquidity
- Third-party, off-chain bot errors (for instance bugs with an arbitrage bot running on the smart contracts)
- Best practice critiques
- Sybil attacks
- Attempted phishing or other social engineering attacks involving Drift contributors or users
- Denial of service, or automated testing of services that generate significant traffic.
- Any submission violating Immunefi's rules

Audits Risks