Beanstalk

[dd.mm.yyyy]	**No**	**USD 1 100 000**
Live since	KYC Required	Max Bounty

Program Overview

Beanstalk is a permissionless fiat stablecoin protocol built on Ethereum.

Beanstalk forms the monetary basis of an Ethereum-native, rent-free economy facilitated by the positive carry of its native fiat currency, a stablecoin called Bean.

For more information about Beanstalk, please visit https://bean.money/.

This bug bounty program is focused on the Beanstalk smart contracts and preventing the loss of user funds.

Rewards by Threat Level

Rewards are distributed according to the impact of the vulnerability based on the Immunefi Vulnerability Severity Classification System V2.2. The following is a simplified 3-level scale, focusing on the impact of the vulnerability reported. The complete scope can be found below.

Smart Contracts

Critical	**USD 100 000 up to USD 1 100 000**
High	**USD 10 000 up to USD 100 000**
Medium	**USD 1 000 up to USD 10 000**

In order to be considered for the maximum potential reward, bug reports must come with (1) a Proof of Concept (PoC), and (2) code implementing the fix. Explanations and statements are not accepted in lieu of a PoC and code implementing the fix. Bug reports that do not come with a PoC and code implementing a fix may qualify for a maximum of up to 30% of the potential reward outlined below, as determined by the Beanstalk Immunefi Committee (or BIC, see BIP-26).

Rewards for Critical smart contract vulnerabilities are capped at the *lower* of (a) 10% of practicable economic damage, or (b) **USD 1 100 000**, primarily taking into consideration funds at risk. However, there is a minimum reward of **USD 100 000** for Critical severity smart contract bug reports.

Rewards for High smart contract vulnerabilities are capped at the *lower* of (a) 100% of practicable economic damage, or (b) **USD 100 000**, primarily taking into consideration funds at risk. However, there is a minimum reward of **USD 10 000** for High severity smart contract bug reports.

Rewards for Medium severity smart contract vulnerabilities are scaled based on a set of internal criteria established by Beanstalk Farms. However, there is a minimum reward of **USD 1 000** for Medium smart contract bug reports. Beanstalk Farms will primarily take into account:
- The exploitability of the bug;
- The impact it causes; and

- The likelihood of the vulnerability presenting itself.

Payouts are handled by the Beanstalk Community Multisig (BCM) directly and are done in BEAN at the rate of 1 BEAN to 1 USD (*i.e.*, amounts listed above are actually in BEAN).

All vulnerabilities noted in any Halborn audit reports or the Trail of Bits audit report (or otherwise known by the BIC or BCM) are not eligible for a reward.

BIP-26 formed the BIC. The BIC shall determine whether a submitting party is entitled to a bug bounty/reward, and if so, the amount of such bounty/reward (and specifically, whether such submission qualifies for a Critical, High or Medium Impact bounty/reward, what is the potential practicable economic damage of such bug, and what the appropriate bounty/reward should be within each Impact range). The BIC's determination of (i) whether such submission qualifies for a Critical, High or Medium Impact bounty/reward, (ii) what is the potential practicable economic damage of such bug, and (iii) whether such submission came with a PoC and code implementing a fix, thereby enabling it to be considered for the maximum potential applicable reward (vs. a submission that did not come with a PoC and code implementing a fix, thereby limiting such submission to a maximum of up to 30% of the applicable reward), shall be made in the BIC's sole and absolute discretion absolute and shall be final, and not be subject to any appeal or challenge.

A submitting party may only dispute the BIC's determination (a) that a submitting party is not entitled to any bug bounty/reward, or (b) what the appropriate bounty/reward should be within each Impact range. In such disputes, Immunefi will conduct a binding mediation. If the submitting party disputes the BIC's decision that a submitting party is not entitled to any bug bounty/reward, Immunefi will mediate, and shall determine, in its sole and absolute discretion, which is non-appealable, whether the submitting party is entitled to any bug bounty/reward, and if so, the amount of such bug bounty/reward, up to **USD 10 000** (i.e., as if it were a Medium Impact fix). If the submitting party disputes the BIC's determination what the appropriate bounty/reward should be within a specific Impact range, Immunefi will mediate, and shall determine, in its sole and absolute discretion, which is non-appealable, the amount of such bug bounty/reward in the relevant Impact category; however, Immunefi may not modify or change (i) the practicable economic damage determination made by the BIC, or (b) the BIC's determination whether such submission came with a PoC and code implementing a fix, thereby enabling it to be considered it for the maximum potential applicable reward (vs. a submission that did not come with a PoC and code implementing a fix, thereby limiting such submission to a maximum of up to 30% of the applicable reward).

Assets in Scope

Target	Type
https://etherscan.io/address/0xBEA0000029AD1c77 D3d5D23Ba2D8893dB9d1Efab	Smart Contract - Bean ERC-20 token
https://etherscan.io/address/0x1BEA0050E63e05FB b5D8BA2f10cf5800B6224449	Smart Contract - Unripe Bean ERC-20 token
https://etherscan.io/address/0x1BEA3CcD22F4EBd 3d37d731BA31Eeca95713716D	Smart Contract - Unripe BEAN:3CRV LP ERC-20 token
https://etherscan.io/address/0x402c84de2ce49af88f	Smart Contract - Fertilizer ERC-1155 token

[5e2ef3710ff89bfed36cb6](#)	
[https://etherscan.io/address/0xC1E088fC1323b20B CBee9bd1B9fC9546db5624C5](https://etherscan.io/address/0xC1E088fC1323b20BCBee9bd1B9fC9546db5624C5)	Smart Contract - Beanstalk
[https://etherscan.io/address/0x39cdAf9Dc6057Fd7A e81Aaed64D7A062aAf452fD](https://etherscan.io/address/0x39cdAf9Dc6057Fd7Ae81Aaed64D7A062aAf452fD)	Smart Contract - Fertilizer Implementation

All Beanstalk smart contracts can be found at https://github.com/BeanstalkFarms/Beanstalk. However, only those in the *Assets in Scope* section are considered as in-scope of the bug bounty program.

Though only the current facets are listed as in-scope, the current implementation and any further updates to the contracts are considered in-scope. When reporting a bug, please make sure to select the relevant smart contract as the target.

If an impact can be caused to any other asset related to Beanstalk that isn't on this section but for which the impact is in the *Impacts in Scope* section below, bug bounty hunters are encouraged to submit it for consideration by Beanstalk Farms.

Impacts in Scope

Only the following impacts are accepted within this bug bounty program. All other impacts are not considered as in-scope, even if they affect something in the *Assets in Scope* section.

Smart Contracts

Critical
- Any governance voting result manipulation;
- Direct theft of any user funds, whether at-rest or in-motion, other than unclaimed yield; and
- Permanent freezing of funds.

High
- Theft of unclaimed yield;
- Permanent freezing of unclaimed yield;
- Temporary freezing of funds for at least 1 hour; and
- Illegitimate minting of protocol native assets.

Medium
- Smart contract unable to operate due to lack of token funds;
- Block stuffing for profit;
- Griefing (*e.g.*, no profit motive for an attacker, but damage to the users or the protocol);
- Theft of gas;
- Unbounded gas consumption; and
- Smart contract fails to deliver promised returns, but doesn't lose value.

Out of Scope & Rules

The following vulnerabilities are excluded from the rewards for this bug bounty program:

- Attacks that the reporter has already exploited themselves, leading to damage;
- Attacks requiring access to leaked keys/credentials; and
- Attacks requiring access to privileged addresses (governance, strategist).

Smart Contracts

- Incorrect data supplied by third party oracles;
    - Not to exclude oracle manipulation/flash loan attacks;
- Basic economic governance attacks (*e.g.*, 51% attack);
- Lack of liquidity;
- Best practice critiques;
- Sybil attacks; and
- Centralization risks.

Prohibited Activities

The following activities are prohibited by this bug bounty program and could result in disqualification of reception of a bounty, in the sole and absolute discretion of Beanstalk Farms:

- Any testing with mainnet or public testnet contracts; all testing should be done on private testnets;
- Any testing with pricing oracles or third party smart contracts;
- Attempting phishing or other social engineering attacks against our contributors and/or users;
- Any testing with third party systems and applications (*e.g.*, browser extensions) as well as websites (*e.g.*, SSO providers, advertising networks);
- Any denial of service attacks;
- Automated testing of services that generates significant amounts of traffic
- Public disclosure of an unpatched vulnerability in an embargoed bounty.