Beanstalk Immunefi Program

Live since	KYC required	Maximum bounty
11 October 2022	No	$1,100,000

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 primarily focused on preventing the loss of Farmers' Beanstalk-native assets within Beanstalk and other ecosystem smart contracts.

Resources:

- Beanstalk on Louper, the Ethereum Diamond Inspector;
- The Beanstalk contract on GitHub;
- The Agronomics Handbook (technical documentation);
- Past bug reports and past bounty payouts; and
- The Beanstalk Discord — bring questions to the **#development** channel!

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**

Website and Applications

- Critical — **USD 5 000 up to USD 50 000**
- High — **USD 1 000 up to USD 5 000**

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. Given that the focus of the bug bounty program is Beans/BDV at risk, Circulating non-Bean assets at risk may qualify for a maximum of up to 50% of the potential reward outlined below, as determined by the BIC.

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 Beans/BDV 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 Beans/BDV 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 and all website and applications vulnerabilities are scaled based on a set of internal criteria established by the BIC. However, there is a minimum reward of **USD 1 000** for Medium smart contract bug reports, **USD 5 000** for Critical website and applications bug reports and **USD 1 000** for High website and applications bug reports. The BIC 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 audit report in the Beanstalk Audits repository (or otherwise known by the BIC, BCM, or Root DAO Multisig) are not eligible for a reward.

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 based on the Beans/BDV at risk, 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 based on the Beans/BDV at risk, 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** in the case of a smart contract bug reports (i.e., as if it were a Medium Impact fix), and up to **USD 1 000** in the cases of a website and applications bug report (i.e., as if it were a High 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/0xBEA0000029AD1c77D3d5D23Ba2D8893dB9d1Efab	Smart Contract - Bean ERC-20 token
https://etherscan.io/address/0x1BEA0050E63e05FBb5D8BA2f10cf5800B6224449	Smart Contract - Unripe Bean ERC-20 token
https://etherscan.io/address/0x1BEA3CcD22F4EBd3d37d731BA31Eeca95713716D	Smart Contract - Unripe BEAN:3CRV LP ERC-20 token
https://etherscan.io/address/0x402c84de2ce49af88f5e2ef3710ff89bfed36cb6	Smart Contract - Fertilizer ERC-1155 token
https://etherscan.io/address/0xC1E088fC1323b20BCBee9bd1B9fC9546db5624C5	Smart Contract - Beanstalk
https://etherscan.io/address/0x39cdAf9Dc6057Fd7Ae81Aaed64D7A062aAf452fD	Smart Contract - Fertilizer Implementation
https://etherscan.io/address/0xb1bE0000bFdcDDc92A8290202830C4Ef689dCeaa	Smart Contract - Pipeline
https://etherscan.io/address/0xDEb0f000082fD56C10f449d4f8497682494da84D	Smart Contract - Depot
https://etherscan.io/address/0x77700005bea4de0a78b956517f099260c2ca9a26	Smart Contract - Root ERC-20 token
https://app.bean.money	Website and Applications - Beanstalk UI

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 the BIC.

Note that unexpected outcomes (like loss of funds) due to misuse of Pipeline do not qualify as valid bug reports. Read more here.

Undeployed Code in Scope

The BIC also maintains a list of pull requests/repositories whose code is considered in-scope but has not yet been deployed on-chain. This code has been audited. The following code is in-scope of the bug bounty program:

- None at this time.

Links

All Beanstalk smart contracts and the UI 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. The following links may also be helpful:

- Beanstalk Whitepaper
- Beanstalk Docs
- Root Whitepaper
- Root Docs
- Root GitHub
- Pipeline Whitepaper
- Pipeline GitHub

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.

Website and Applications

Critical

- Taking down the application/website requiring manual restoration;
- Redirecting users to malicious websites;
- Direct theft of user funds;
- Ability to execute arbitrary system commands;
- Injecting code that results in malicious interactions with an already-connected wallet such as modifying transaction arguments or parameters, substituting contract addresses, submitting malicious transactions; and
- Taking state-modifying authenticated actions (with or without blockchain state interaction) on behalf of other users without any interaction by that user, such as voting in governance.

High

- A temporary or self-correcting loss of website availability (e.g. a mitigatable vulnerability to DDoS)
- Lack of valid SSL/TLS;
- Subdomain takeover other than app.bean.money; and
- Persistent content spoofing / text injection issues.

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.

Website and Applications

- Theoretical vulnerabilities without any proof or demonstration;
- Self-XSS;
- CSRF with no security impact (logout CSRF, change language, etc.);
- Missing HTTP Security Headers (such as X-FRAME-OPTIONS) or cookie security flags (such as “httponly”);
- Server-side information disclosure such as IPs, server names, and most stack traces;
- Vulnerabilities requiring unlikely user actions;
- A non-mitigatable DDoS vulnerability;
- Feature requests;
- Best practices issues without concrete impact and PoC;
- Vulnerabilities primarily caused by browser/plugin defects;
- Leakage of non sensitive API keys such as Etherscan, Infura, Alchemy, etc.;
- Any vulnerability exploit requiring CSP bypass resulting from a browser bug;
- Vulnerabilities that require compromise of the user’s machine / browser; and
- Clickjacking vulnerabilities.

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 the BIC:

- 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; and
- Public disclosure of an unpatched vulnerability in an embargoed bounty.