SIP-0008: Sovryn Bug Bounty Program

Summary

Immunefi proposes the creation of a bug bounty program, to be funded by the Sovryn treasury, to incentivize the discovery and discreet disclosure of vulnerabilities in specified parts of the Sovryn platform.

Immunefi Overview

Immunefi is a bug bounty platform focused around cryptocurrencies created with the intention of preventing catastrophic hacks around the space and making security more accessible. It offers this service with a pure performance fee basis with no costs related to onboarding, maintenance, or other modifications, nor requires any deposit to our wallets. With a bug bounty program with high enough bounty payouts, Immunefi believes that it can even economically incentivize black hat hackers to disclose a bug instead of exploiting it, due to the difficulties associated with dealing with stolen funds. In addition to the bug bounty platform, Immunefi also offers premium bug report triaging and management, leveraging its expertise to handle the bug report management process.

Immunefi has a growing community of white hat hackers that have been successful in finding, disclosing, then assisting to repair catastrophic vulnerabilities, including one which got covered on CoinDesk, leading to a positive reputation boost for the project as well as increased confidence in the platform by the community.

Program overview

The Sovryn bug bounty program will be focused around its smart contracts and app and the prevention of the loss of user funds, either by loss of access or by direct theft, as well as accessibility to the app. A full list of what will be covered is listed under Assets in Scope. Upon the advice of the Sovryn team, this list may be expanded to further secure other assets.

During the initial phase of the bug bounty program, the program will add bonuses to the payout amount for bugs reported within the bonus period as well as will work with Sovryn to provide NFT rewards for validated Critical and High level bug reports.

Immunefi will also provide its premium bug report triaging and management service and thus handle and receive all bug report submissions, freeing up the Sovryn team to focus on other tasks while only having to deal with bug reports that have been validated by the moderation team as well as not have to worry about spending time interacting with the bug reporters themselves. Full coordination with public relations with regards to recognition of a patched vulnerability that was due to a bug report through Immunefi will also be provided. However, though the moderation team will provide its recommendations, the final decision on the severity level and the payout will be with the Sovryn team itself.

Fee Structure for Immunefi

For the bug bounty platform itself, Immunefi will only take a 10% fee on top of the reward paid out to the bug reporter after Sovryn has sent out the reward. This fee will not reduce the reward the bug reporter receives and they will receive the full displayed amount.

For the bug report triaging and management service, it will start at the current experimental rate of USD 1000 per month for the first ten submitted bug reports of that month, with a succeeding addition of USD 1000 per month for another 10 bug reports consumable for the same month, for every time it goes above the allocated number of reports. These fees however, are payable in BTC. If a month has less than or equal to three bug reports in a given month, there will not be a fee charged but instead the total will be carried over to the succeeding month. Additionally, if the tranche of 10 is completed and another tranche is started, but the number of bug reports is less than or equal to 3, that total is carried over to the succeeding month and the initial month only gets charged USD 1000. If a month has 0 bug reports, there is no fee charged. ~~Bug reports that are considered spam, e.g copyright date issues, are not counted.~~ In addition to obvious unacceptable reports, such as UX issues, feature requests, documentation errors, typos, copyright date issues, and out-of-scope reports (including those that at first glance are not within a paid tier of vulnerability severity), all incomplete reports are not counted until a reviewable report is sent.

To keep costs under control, a group will be set up on Keybase (or Discord if preferred) for active communication regarding the bugs that are being submitted so we can quickly make adjustments as needed (e.g pausing web/app bug reports, having some reports just go directly to the Sovryn team, etc.). Additionally, going above $2k (up to 20 bug reports) in any month requires approval from the Sovryn team on that channel to increase beyond that.

Rewards by threat level

Rewards are distributed according to the impact of the vulnerability based on the Immunefi Vulnerability Severity Classification System. This is a simplified 5-level scale, with separate scales for websites/apps and smart contracts/blockchains, encompassing everything from consequence of exploitation to privilege required to likelihood of a successful exploit.

Smart Contracts and Blockchain

Severity Level	Payout	USD Estimate
Critical*	Up to 18 BTC	Up to USD 1 000 000
High	0.5 BTC	USD 22 140
Medium	0.2 BTC	USD 8 800
Low	0.05 BTC	USD 2 200

*For Critical bugs, the payout amount is capped at 10% of the funds at risk.

Website/App

Severity Level	Payout	USD Estimate
Critical	0.5 BTC	USD 22 140
High	0.2 BTC	USD 8 800
Medium	0.05 BTC	USD 2 200
~~Low~~	~~0.01 BTC~~	~~USD 440~~

All payouts are done in BTC and payouts are pegged to those amounts. The USD Estimate column is provided just as a guide.

Bonus Countdown

Until the end of the bonus period, Sovryn will provide bonuses for **Smart Contract/Blockchain** bug reports based on the remaining time of the bonus period. In addition, **critical and high Smart Contract/Blockchain** bug reports that are validated will receive a unique artwork NFT on Sovryn, showing them as the heroes that they are, all throughout the bonus period. These NFTs will be designed upon each accepted Smart Contract/Blockchain high and critical bug reports.

Bonus Time Remaining	Bonus
More than 3 weeks	+25%
Between 2 and 3 weeks	+20%
Between 1 and 2 weeks	+15%
Less than a week	+10%

Payouts are handled by **Sovryn** directly and are done in BTC as well as based in it. However, the Sovryn team may decide to have up to 50% of the payment in SOV, which may include a vesting schedule.

In the case of Critical bugs that are affected by the 10% cap, the bonus will be applied after the cap.

~~**Bonus Easter Eggs**~~

~~Sovryn wants to reward the bug bounty hunters for looking through the code, even if they don't find any bugs. Depending on the easter egg found, a corresponding unique NFT will be provided on a first-come-first served basis. There are a total of TBD easter eggs found in the Smart Contract code. Happy hunting!~~

Immunefi Promotion

Throughout the bonus period, Immunefi will provide exposure for the Sovryn bug bounty program, in addition to the initial launch promotion consisting of an announcement on Twitter, on Discord, and the email newsletter. This includes:

- A standalone newsletter blast focusing only on the Sovryn bug bounty program
- A tweet each day during the first week of the bonus period
- At least two tweets per week during the bonus period (one tweet indicating the change and the other indicating that it's about to be over and the bonus amount further reduced)
- At least one announcement per week on the Discord channel
- Travin (@TravinKeith) will personally RT and Like all Sovryn-related tweets from the Immunefi account, will follow the Sovryn Twitter account (already done), and do the same for bug bounty-related tweets from the Sovryn Twitter account
- A countdown clock on the Sovryn bug bounty page.
- A countdown clock on the homepage under the Sovryn bug bounty program row.

Like with all critical bug reports that are accepted by Immunefi's clients, we will work with the Sovryn team in order to maximize positive PR in order to drive further confidence in the platform's security due to a patch that wasn't exploited, as well as to further highlight that experts are looking through the Sovryn codebase.

Additional Promotion

Based on feedback from the Sovryn community, an ad of the bug bounty program on Gitcoin, which would be a regular bounty program though with a minimal prize. The information on Gitcoin will be a light overview of the bug bounty program and then information indicating that they should submit bug reports through the Immunefi bug bounty platform.

Assets in Scope

Target	Type
https://github.com/DistributedCollective/Sovryn-smart-contracts	Smart Contract
https://github.com/DistributedCollective/Sovryn-frontend	App - Front-end

https://github.com/DistributedCollective/multisig-ui	App - Multisig UI
https://github.com/DistributedCollective/governance-dapp	App - Governance
https://live.sovryn.app/	Website/App

For web/app bug reports, only those that directly affect the assets in scope are accepted.

Prioritized vulnerabilities

We are especially interested in receiving and rewarding vulnerabilities of the following types:

Smart Contracts/Blockchain

- Re-entrancy
- Logic errors
    - including user authentication errors
- Solidity/EVM details not considered
    - including integer over-/under-flow
    - including unhandled exceptions
- Trusting trust/dependency vulnerabilities
    - including composability vulnerabilities
- Oracle failure/manipulation
- Novel governance attacks
- Economic/financial attacks
    - including flash loan attacks
- Congestion and scalability
    - including running out of gas
    - including block stuffing
    - including susceptibility to frontrunning
- Consensus failures
- Cryptography problems
    - Signature malleability
    - Susceptibility to replay attacks
    - Weak randomness
    - Weak encryption
- Susceptibility to block timestamp manipulation
- Missing access controls / unprotected internal or debugging interfaces

Website/App

- Remote Code Execution
- Trusting trust/dependency vulnerabilities

- Vertical Privilege Escalation
- XML External Entities Injection
- SQL Injection
- LFI/RFI
- Horizontal Privilege Escalation
- Stored XSS
- Reflective XSS with impact
- CSRF
- CSRF with impact
- Direct object reference
- Internal SSRF
- Session fixation
- Insecure Deserialization
- Direct object reference
- Path Traversal
- DOM XSS
- SSL misconfigurations
- SPF configuration problems
- SSL/TLS issues (weak crypto, improper setup)
- URL redirect
- Clickjacking
- Misleading Unicode text (e.g. using right to left override characters)
- Coercing the application to display/return specific text to other users

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
- Attacks requiring access to privileged addresses (governance, strategist)

Smart Contracts and Blockchain

- 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

Websites and Apps

- Theoretical vulnerabilities without any proof or demonstration
- Content spoofing / Text injection issues
- Self-XSS

- Captcha bypass using OCR
- 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 used to enumerate or confirm the existence of users or tenants
- Vulnerabilities requiring unlikely user actions
- URL Redirects (unless combined with another vulnerability to produce a more severe vulnerability)
- Lack of SSL/TLS best practices
- DDoS vulnerabilities
- Attacks requiring privileged access from within the organization
- Feature requests
- Best practices

The following activities are prohibited by bug bounty program:

- 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 employees and/or customers
- 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

In the case of two or more reports covering the same vulnerability, only the first complete bug report gets the reward.

Total Funds Requested

For the bug bounty component, we request the allocation of enough BTC to cover up to 1 validated critical bug reports at full value, plus the 10% fee for Immunefi, payable upon accepted bug report. This comes to a total of **BTC 25**. Throughout the bonus period, additional funds will be allocated when payouts occur in order to ensure that there will be enough funds to cover the full payment of a maximum critical bug report. At the end of the bonus period, a one-time reallocation addition to BTC 25 will occur, in order to be able to cover at least one maximum critical bug report.

Recipient address and management of funds: Sovryn Treasury Multisig. No funds will be transferred to Immunefi as a deposit. The only time funds will be transferred will be to pay the bug reporters, directly from the treasury, and then to Immunefi.

For the bug report triaging and management service, we request the allocation of enough BTC to cover up to 20 bug reports per month for six months at the rate mentioned. This comes to a total of **USD 12 000**, payable in BTC. However, this amount is simply a consumable amount depending on the amount of bugs submitted and not to be paid upfront. If further funds are needed, either for the continuation of the service or because of the volume of bug reports coming in, a separate proposal will be created.

Immunefi Accountability

Immunefi will post a monthly report of the work that was done while the bug report triaging and management service is in place. This report will first be sent to the Sovryn development team before public posting on the Sovryn forum in order to ensure that bug reports they wish to temporarily keep under embargo will remain confidential until it is safe to disclose publicly.