Verse NFT Audit Report

Audited by:
jokr
sh15h4nk

April 18, 2024

Contents

Executive Summary

Verse NFT is a contract that mints NFT characters for users. These characters can possess various traits such as body type, color, and gear etc. The contract integrates Chainlink VRF to randomly assign these traits during character creation. Users have the option to reroll specific traits to customize their characters further.

Audit scope

Repository:

https://github.com/bitcoin-verse/verse-nft-audit

Contracts:

contracts/ReelVRF.sol
contracts/ReelNFT.sol
contracts/CommonNFT.sol
contracts/CommonVRF.sol

Risk classification

Impact:

- High - Funds are directly at risk, or a severe disruption of the protocol core functionality
- Medium - Funds are indirectly at risk, or some disruption of protocol's functionality
- Low - Funds are at no risk

Likelihood:

- Almost certain to happen, easy to perform, or not easy but highly incentivised
- Only conditionally possible or incentivised, but still relatively likely
- Low - Very unlikely to happen, or little-to-no incentive

Findings

[M-1] Users get unusable NTFs in case of pending randomness requests deleted

Description:

Randomness requests can go into pending state, if subscription is low in funds. These requests will be deleted in 24 hours if no funds are added.

In such cases, the NFT will already have been minted by `_mintCharacter`. However, since the request is never processed, the minted NFT will remain without traits. Even if a user attempts to reroll traits for this NFT, it is not possible due to the following check in `rerollTrait`:

```
if (results[_astroId][_traitId] == 0) {
    revert TraitNotYetDefined();
}
```

Similarly, once an NFT has been minted, if any request to reroll a trait is not fulfilled, users will not have another opportunity to further reroll traits to their NFT. Because once a reroll is in progress, no other rerolls are allowed for the specific NFT.

```
if (rerollInProgress[_astroId] == true) {
    revert RerollInProgress();
}
```

References:

https://github.com/bitcoin-verse/verse-nft-audit/blob/main/contracts/ReelVRF.sol#L279-L281

https://github.com/bitcoin-verse/verse-nft-audit/blob/main/contracts/ReelVRF.sol#L283-L285

Impact: Medium

Users get unusable NFTs for base cost. In the second case users will not be able to customize their NFTs further

Likelihood: Low

Admin is responsible for monitoring funds in the subscription. So chances of this happening are very unlikely.