SOLIDIFIED

Audit Report for Animoca Core Library Extension - Oct 18, 2023

Summary

Audit Report prepared by Solidified covering the Animoca Core Library Extension smart contracts.

Process and Delivery

Three (3) independent Solidified experts performed an unbiased and isolated audit of the code below. The final debrief took place on Oct 18, 2023, and the results are presented here.

Intended Behavior

Animoca Core Library is a Solidity contracts development library.

SOLIDIFIED

Audit Report for Animoca Core Library Extension - Oct 18, 2023

Audited Files

The source code has been supplied in a public source code repository:

https://github.com/animoca/ethereum-contracts/
Commit number: `f609f2d975ff4c5121aef3265c2891b959105ef4`

Scope:
```
/contracts/token/metadata/libraries/TokenMetadataStorage.sol
/contracts/token/metadata/base/TokenMetadataBase.sol
/contracts/token/metadata/TokenMetadataResolverPerToken.sol
/contracts/token/metadata/TokenMetadataResolverRandomizedReveal.sol
/contracts/token/metadata/TokenMetadataResolverWithBaseURI.sol
/contracts/token/ERC721/base/ERC721MetadataBase.sol
/contracts/token/ERC721/facets/ERC721MetadataFacet.sol
/contracts/token/ERC721/ERC721Metadata.sol
/contracts/token/ERC721/preset/ (all contracts in folder)
/contracts/token/ERC721/preset/proxied/ (all contracts in folder)
/contracts/token/ERC1155/ERC1155Metadata.sol
/contracts/token/ERC1155/facets/ERC1155MetadataFacet.sol
/contracts/token/ERC1155/base/ERC1155MetadataBase.sol
/contracts/token/ERC1155/preset/ (all contracts in folder)
/contracts/token/ERC1155/preset/proxied/ (all contracts in folder)
```

Update: The team provided fixes on October 23, 2023.
Commit number: `fa9ca10004562eed33e9ac1ed316a2d8342b1c02`

Findings

Smart contract audits are an important step to improve the security of smart contracts and can find many issues. However, auditing complex codebases has its limits and a remaining risk is present (see disclaimer).

Users of a smart contract system should exercise caution. In order to help with the evaluation of the remaining risk, we provide a measure of the following key indicators: **code complexity**, **code readability**, **level of documentation**, and **test coverage**.

Note, that high complexity or lower test coverage does not necessarily equate to a higher risk, although certain bugs are more easily detected in unit testing than a security audit and vice versa.

Criteria	Status	Comment
Code complexity	Low	-
Code readability and clarity	High	-
Level of Documentation	High	-
Test Coverage	High	-

SOLIDIFIED

Audit Report for Animoca Core Library Extension - Oct 18, 2023

Issues Found

Solidified found that the Animoca Core Library V2 contracts contain no critical issues, no major issues, 1 minor issue, and 2 informational notes.

We recommend issues are amended, while informational notes are up to the team's discretion, as they refer to best practices.

Issue #	Description	Severity	Status
1	TokenMetadataResolverRandomizedReveal.sol: Function _requestReveal() does not revert on RevealStatus.Requested	Minor	Acknowledged
2	TokenMetadataResolverPerToken.sol: Missing events	Note	Resolved
3	Documentation typos	Note	Resolved

Critical Issues

No critical issues have been found.

Major Issues

No major issues have been found.

Minor Issues

1. TokenMetadataResolverRandomizedReveal.sol: Function _requestReveal() does not revert on RevealStatus.Requested

The `_requestReveal()` function only reverts on `RevealStatus.Revealed`, but does not revert on `RevealStatus.Requested`. This could be problematic since users can request reveal multiple times, however, once `VRF_V2_WRAPPER.rawFulfillRandomWords()` is called, the `offset` is set and the function cannot be re-executed. This would lead to loss of funds for users requesting multiple reveals before the completion of their initial request.

Recommendation

Revert on both `RevealStatus.Revealed` and `RevealStatus.Requested`.

Status

Acknowledged. Team's response: "*This is a feature rather than an issue. If the reveal fails for any reason, it is necessary to be able to retry by pushing a new request*".

Informational Notes

2. TokenMetadataResolverPerToken.sol: Missing events

Consider emitting events on `setTokenURI()` and `batchSetTokenURI()`.

Status

Resolved

3. Documentation typos

The following files contain documentation typos:

- `TokenMetadataResolverRandomizedReveal.sol:106`
- `TokenMetadataResolverRandomizedReveal.sol:108`

Status

Resolved

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of Animoca or its products. This audit does not provide a security or correctness guarantee of the audited smart contract. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

The individual audit reports are anonymized and combined during a debrief process, in order to provide an unbiased delivery and protect the auditors of Solidified platform from legal and financial liability.

Oak Security GmbH