Supra Smart Contract

Audit Report

contact@bitslab.xyz

https://twitter.com/movebit_

Sun Sep 10 2023

Supra Smart Contract Audit Report

1 Executive Summary

1.1 Project Information

Description	An Oracle on Aptos
Type	Oracle
Auditors	MoveBit
Timeline	Mon Aug 28 2023 - Thu Sep 07 2023
Languages	Move
Platform	Aptos
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/Entropy-Foundation/supra-contracts
Commits	2ecf8c72fcf4b02f89ef55488f66d02d23dd9947 3256a8f683fc5104b73a3cad1c6840f6512f9af0 d31e3e6bb574d9d5093ab523e4012c46cd899f73

1.2 Files in Scope

The following are the SHA1 hashes of the original reviewed files.

ID	File	SHA-1 Hash
MOV	move/svalue/with_verification/decentralized/Move.toml	a9e7d20f025e1731c1e0b1310ef02712d97c06ae
SUT	move/svalue/with_verification/decentralized/sources/supra_util.move	786b5c7b829d6a7634071fcea7fd88179f8cece4
SSVF	move/svalue/with_verification/decentralized/sources/SupraSValueFeed.move	95698c490211c6d3f2336ec94a68762a9daa0664

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	3	3	0
Informational	0	0	0
Minor	2	2	0
Medium	1	1	0
Major	0	0	0
Critical	0	0	0

1.4 MoveBit Audit Breakdown

MoveBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues our team looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow by bit operations
- Number of rounding errors
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting
- Unchecked CALL Return Values
- The flow of capability
- Witness Type

1.5 Methodology

The security team adopted the **"Testing and Automated Analysis"**, **"Code Review"** and **"Formal Verification"** strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are stated in the conventions in the "Audit Objective", which can expand to contexts beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

(2) Code Review

The code scope is illustrated in section 1.2.

(3) Formal Verification

Perform formal verification for key functions with the Move Prover.

(4) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time. The code owners should actively cooperate (this might include providing the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in a timely manner.

2 Summary

This report has been commissioned by Entropy Foundation to identify any potential issues and vulnerabilities in the source code of the Supra smart contract, as well as any contract dependencies that were not part of an officially recognized library. In this audit, we have utilized various techniques, including manual code review and static analysis, to identify potential vulnerabilities and security issues.

During the audit, we identified 3 issues of varying severity, listed below.

ID	Title	Severity	Status
SSV-1	Missing Length Validation Assertions for Vector-Type Parameters in the `process_cluster` Function	Minor	Fixed
SSV-2	Inefficient Assignment Within Loop in the `process_cluster` Function	Medium	Fixed
SSV-3	Unused Constant	Minor	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the Supra Smart Contract :

Admin

- Admin can update the public key of the `DkgState` resource through `update_public_key()` .

Free Node

- Free Node can update the price feed for respective pairs through `process_cluster()`

User

- User can get the `priceFeedData` value for that particular trading Pair and multiple trading Pair through `get_price()` and `get_prices()` .

4 Findings

SSV-1 Missing Length Validation Assertions for Vector-Type Parameters in the `process_cluster` Function

Severity: Minor

Status: Fixed

Code Location:

move/svalue/with_verification/decentralized/sources/SupraSValueFeed.move#234

Descriptions:

It is essential to ensure that the lengths of all Vector-type parameters are consistent within the `process_cluster` function; otherwise, it may result in an abort. However, there is a lack of assertions for validating the lengths of Vector-type parameters.

Suggestion:

It is recommended to insert assertions to verify that their lengths are consistent before any critical data processing involving Vector-type parameters.

Resolution:

The client followed our suggestion and fixed this issue.

SSV-2 Inefficient Assignment Within Loop in the `process_cluster` Function

Severity: Medium

Status: Fixed

Code Location:

move/svalue/with_verification/decentralized/sources/SupraSValueFeed.move#316

Descriptions:

During the analysis of the codebase, it was identified that the assignment operation located at line 316 within the `process_cluster` function is unnecessarily repeated in every iteration of the loop. This will result in less efficient execution and increased gas consumption.

Suggestion:

It is recommended to move this assignment code to a position immediately before the loop, ensuring that the assignment is performed only once.

Resolution:

The client followed our suggestion and fixed this issue.

SSV-3 Unused Constant

Severity: Minor

Status: Fixed

Code Location:

move/svalue/with_verification/decentralized/sources/SupraSValueFeed.move#27

Descriptions:

The constant `EOWNER` is not used in the contract.

Suggestion:

It is recommended to remove the unused constant.

Resolution:

The client followed our suggestion and fixed this issue.

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Partially Fixed:** The issue has been partially resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

Appendix 2

Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.