Supra V2

Audit Report

MOVEBIT

contact@bitslab.xyz

https://twitter.com/movebit_

Mon Jun 17 2024

Supra V2 Audit Report

1 Executive Summary

1.1 Project Information

Description	Supra V2 is the second version of the oracle contracts.
Type	Oracle
Auditors	MoveBit
Timeline	Mon May 13 2024 - Mon Jun 17 2024
Languages	Solidity
Platform	Sui,Aptos
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/Entropy-Foundation/supra-contracts/
Commits	2996c6bea2e4b799c63c263f25f34c26db53c449 7565f92051f329c78faa0608ee92771df29b3d73

1.2 Files in Scope

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

ID	File	SHA-1 Hash
CAR	move/svalue/without_verification/Cargo.toml	15ead16cafa8948798c7ed03f3f64c6adfe31a65
MOV	move/svalue/without_verification/Move.toml	3de015f391ecaa7a9c4fe5133c36b5de16666ee6
SPO	move/svalue/without_verification/sources/SupraPriceOracle.move	7c489d0e2dea5e63c99c4df45ec22672ea868709
MOV	move/svalue/with_verification/decentralized/Move.toml	a9e7d20f025e1731c1e0b1310ef02712d97c06ae
MOV	move/svalue/with_verification/supra-svalue-feed-framework/Move.toml	2817dcdc36f16d9c3944c5e28d021847bcecc467
SSVF	move/svalue/with_verification/supra-svalue-feed-framework/sources/SupraSValueFeed.move	d734d52abcae29aaa32ee323ebe165b39f77d4f0
MOV	move/svalue/with_verification/example/Move.toml	266574746379b35f003a475b378d7bdc0172096f
EXA	move/svalue/with_verification/example/sources/Example.move	beaab5cf2cf38b015fc8446502ee6fda800071ba
MOV	sui/svalue/without_verification/example/developer-smart-contract/Move.toml	21d85d5a757c2395628b7b789b84ca094e4d7dd5
DCO	sui/svalue/without_verification/example/developer-smart-contract/sources/DeveloperContract.move	4de120e3a53ffe0dc9a217fec87a7405b9b00375

MOV	sui/svalue/without_verification/Move.toml	23979b522a65d1dd848e2a7e2dfe036a8d4b25b8
SOR	sui/svalue/without_verification/sources/SupraOracle.move	5f7db258bcddfdc442869961cf39405d4363519c
CAR	sui/svalue/with_verification/decentralized/parse_sui/Cargo.toml	afd63f072ec12f2ecc3eef558de4a3fbe969efc6
SSVF	move/svalue/with_verification/decentralized/sources/SupraSValueFeed.move	447099504c0fd395944d312a6c0540daf79ab833
BCS	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/bcs.move	8274214210eb0abfabadd4b9a6623675fa7b5c88
TYP	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/types.move	ea801e35bc36f17c8858059f72d5a67f4b16adfa
HEX	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/hex.move	fbb751ce6b739801333ca2e7b4ddd9c10f2cacbf
DOF	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/dynamic_object_field.move	142e467a434ba4f547d51adf035e10cceae95094
OBA	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/object_bag.move	c41e5f7f9f46ca924978cd8be737c43b51be84df
VER	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/versioned.move	243562e0d3246927aea8d0b36e9f2265538511f4
MAT	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/depen	5d5550a10b3162a62057ce5526e357affaea123f

	dencies/Sui/math.move	
EVE	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/event.move	f879b25714355912fc77397db17fb7e4673c8080
TAB	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/table.move	b052ab1a22f6398ed864c6464c2612a6110a30a9
VSE	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/vec_set.move	5a7593b001a4cb5f21c74b4509d298f9b692588d
B12	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/bls12381.move	b8fdd4b35ed17b9d2a005a30c075cb453212dc02
HMA	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/hmac.move	2edf037a47030f12e4481315503adc4341e07b22
URL	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/url.move	726a721ddbb48619082540f0e6078dbc326c183a
BOR	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/borrow.move	f48d4518d20d665da5427fc379e891c9a02fdc92
HAS	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/hash.move	ef95fba4b17a306687c814333eda237c7b79f8c1
BAG	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/bag.move	3f6bbf260294b2356a68de274650f4b615b13921
LTA	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/depen	499a354fb90912bfafe8cc594a2cc4b22e1e96ac

	dencies/Sui/linked_table.move	
PQU	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/priority_queue.move	d1ad54e28d13df524d0f3c05784b0219682ea00b
E25	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/ed25519.move	c3dacffd11bdc3010795e86d4cf979f347b53f73
VMA	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/vec_map.move	9cd30b444139d62208920b37b0e2cdddcee00d2b
OTA	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/Sui/object_table.move	90110a0a1d4c39b290b70719e26fb0588d79340f
ADD1	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/address.move	ea5726e241f734041550891059e9cf49a16507d3
BCS1	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/bcs.move	e0fa2565a2b7c8d7f23bff8427dc32015810ebc0
BVE	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/bit_vector.move	667d9ec55a99e90d27d090e9e8131ce35df51f99
DEB	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/debug.move	aba8aca4d3a1801102bf6445c6d103fadebfa0e6
OPT	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/option.move	e45fe072c8b053b5d2ddfb84bf2b8a61789284e4

VEC	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/vector.move	f51ccfeee07f9ef6ac03ac1544a8c0b64e5cce05
STR	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/string.move	2279b1078b77d26f34b23d7ca9906edd2c270811
FP3	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/fixed_point32.move	bc3161d03d83daefdb87b9cd6c2d54805b667008
HAS1	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/hash.move	c965a564b4f243805831d11a21267e87e207d3d5
ASC	yield-optimizer 2/yield-optimizer/build/YieldOptimizer/sources/dependencies/MoveStdlib/ascii.move	62180008e5fa7ecd1acb4c7d3c32935ca7bcbd91
PDP	supra-contracts/move/svalue/with_verification/framework/supra_holder/sources/price_data_pull.move	69f9548704605d0298985185827032d226a1ce5e
SFH	supra-contracts/move/svalue/with_verification/framework/supra_holder/sources/svalue_feed_holder.move	2ab35890ea84cd29a49720add7358f87e83434dd
VAL	supra-contracts/move/svalue/with_verification/framework/supra_validator/sources/validator.move	597981226b7c9f2333e9ad58ec73c01d668a8a9f
UTI	supra-contracts/move/svalue/with_verification/framework/supra_utils/sources/utils.move	970237a41b75da1e0a06395164f42e283c356001
SUT	supra-contracts/move/svalue/with_verification/decentralized/sources/	6b9da91e01c1f6c4232da6ecdf554cd67e990245

	supra_util.move	
DPC	supra-contracts/move/svalue/with_verification/client_example/sources/derived_pair_client.move	fa9905c1ef17960bb6a076076f2cf1ce74793aab
PCL	supra-contracts/move/svalue/with_verification/client_example/sources/pull_client.move	396543c1a41decf808fb82261a19d775e823104a
PCL1	supra-contracts/move/svalue/with_verification/client_example/sources/push_client.move	95d599022c52852a56265c6f6b9b0c92f56d03d4
PDP1	supra-contracts/move/svalue/with_verification/decentralized_im/supra_holder/sources/price_data_pull.move	54ac5572be873b08b53340351171d444a60d3986
PDP2	supra-contracts/sui/svalue/with_verification/framework/supra_holder/sources/price_data_pull.move	3440bca7fdf60cce29857f4738ae52b05bde05dd
SFH2	supra-contracts/sui/svalue/with_verification/framework/supra_holder/sources/svalue_feed_holder.move	de3b8a96c8f220c31663363e26ac981691780394
VAL2	supra-contracts/sui/svalue/with_verification/framework/supra_validator/sources/validator.move	e229143665f14a7a5703061042f3624e6ef6f4e4
UTI2	supra-contracts/sui/svalue/with_verification/framework/supra_utils/sources/utils.move	c7fa90f8a8edd751f2d945ffd521482cc5aa7550
BCS	move/svalue/with_verification/decentralized_im/supra_utils/sources/bcs.move	5b5f3f3e6f8ae4b7c13a4c38014f1d9f76966a90

SSVF3	sui/svalue/with_verification/supra-svalue-feed-framework/sources/SupraSValueFeed.move	38421a0ec9003c296c3dcb947294944c86859964
DPC2	sui/svalue/with_verification/example/sources/derived_pair_client.move	54d62c0c4323adaee7e757fb3a5c7280545c9b3a
PCL5	sui/svalue/with_verification/example/sources/push_client.move	78586b9fef1ed3f4acc3ec0696deef0efb12780d
PDP3	sui/svalue/with_verification/decentralized/sources/price_data_pull.move	0beadebc95b085c46dbe51455d1cc9d3b408fc64
PDP4	sui/svalue/with_verification/supra-svalue-feed-framework/sources/price_data_pull.move	5ce2e1afdbb1454f3981651d5760f5773b00cfa1
PDP5	sui/svalue/with_verification/decentralized_im/supra_holder/sources/price_data_pull.move	e3ac8b4cedb8a3281a746e1de39ae086e51b962e
BCS1	sui/svalue/with_verification/decentralized_im/supra_utils/sources/bcs.move	ba9288237a62e3cbf6cc6a76be76dbf5e4ac0410
MOV19	sui/svalue/with_verification/example/Move.toml	221cbc4a7f9b2286a23ca9f8fe25e550ee0a7d01
PCL4	sui/svalue/with_verification/example/sources/pull_client.move	5f053ee0e803546f9b8c36480f6d9313a56e1e35
MOV1	move/svalue/with_verification/framework/supra_holder/Move.toml	243ff2993a5c5f9b9efd5d445891187b7ff8243d
PDPV2	move/svalue/with_verification/framework/supra_holder/sources/price_data_pull_v2.move	4b6f9fc5b39d193bb8e2f957ddb70d419cea3311

MOV2	move/svalue/with_verification/framework/supra_validator/Move.toml	16cb4e0eeb46c0b98f160415177fbd8524cb3193
VV2	move/svalue/with_verification/framework/supra_validator/sources/validator_v2.move	daf91693d5ba5b71b6c5eea4b80b563be4d58ec2
MOV3	move/svalue/with_verification/framework/supra_utils/Move.toml	e1e210d1e1313fe818ec2aca5092a3e2c70a1038
MOV5	move/svalue/with_verification/client_example/Move.toml	38d1fc289d6fa4e6a1840fde83a83b057be187bf
PCV2	move/svalue/with_verification/client_example/sources/pull_client_v2.move	e1851dd75cd2f9c35eae0515b0798d4aac962a1f
MOV7	move/svalue/with_verification/decentralized_im/supra_holder/Move.toml	f470ab82cb7a11c5613f652edb99e32d6341a4d7
SFH1	move/svalue/with_verification/decentralized_im/supra_holder/sources/svalue_feed_holder.move	60d2d327002b64ed6481ca321378cb6f9397ef0d
PDPV21	move/svalue/with_verification/decentralized_im/supra_holder/sources/price_data_pull_v2.move	638b3cb60b6a0710ddf1b3ce4c48df510c9c294b
MOV8	move/svalue/with_verification/decentralized_im/supra_validator/Move.toml	e8e577fc12f994f877700fd99d7f513b6329f430
VV21	move/svalue/with_verification/decentralized_im/supra_validator/sources/validator_v2.move	ec140321199a25843a6f495b87a591852c9ee976
VAL1	move/svalue/with_verification/decentralized_im/supra_validator/sourc	31c275ff4d1d92c92ed348ea7237647d9df2694c

	es/validator.move	
MOV9	move/svalue/with_verification/decentralized_im/supra_utils/Move.toml	00769b6e9160d86dd75008d0f0d08ae6fa3e65e6
EMA	move/svalue/with_verification/decentralized_im/supra_utils/sources/enumerable_map.move	3279c2ae415648e958f77d442a589381f2430c02
UTI1	move/svalue/with_verification/decentralized_im/supra_utils/sources/utils.move	41e964ff258c3c0ce54627e81a76fb6da274a360
MOV13	sui/svalue/with_verification/framework/supra_holder/Move.toml	4381cb76a20164123ab7dd2486e5c28534a60179
PDPV22	sui/svalue/with_verification/framework/supra_holder/sources/price_data_pull_v2.move	03f80f1579fc01db4ef47a4cace7490e3def227f
MOV14	sui/svalue/with_verification/framework/supra_validator/Move.toml	3449f4b1648c29e8dca7420d4e824aaee67a7e44
VV22	sui/svalue/with_verification/framework/supra_validator/sources/validator_v2.move	eed3539611543453a7cfb3916ee37e16f9168491
MOV15	sui/svalue/with_verification/framework/supra_utils/Move.toml	2e1ec65d62f0318f5a920e6c42aaf5a52a20074b
MOV16	sui/svalue/with_verification/decentralized/Move.toml	7e77a380edd0b9cf3815c9f5a28b1fcc378f205e
PDPV23	sui/svalue/with_verification/decentralized/sources/price_data_pull_v2.move	6d1cc55fa82bc3f1262f662f21ec5eebf6af75cc
SSVF2	sui/svalue/with_verification/decentralized/sources/SupraSValueFeed.move	ddacaf35fdf948bd78899a6aa0fcc1229c2fae16

MOV17	sui/svalue/with_verification/client_example/Move.toml	513eceebc986dd90b1ee87dec32fb9294035e5fc
DPC1	sui/svalue/with_verification/client_example/sources/derived_pair_client.move	7e77c236581e26ccf3b2072513bb46ce8a518d7f
PCV21	sui/svalue/with_verification/client_example/sources/pull_client_v2.move	fa14d3dd7ac6f4d240acba7262b4aec515e6a07a
PCL2	sui/svalue/with_verification/client_example/sources/pull_client.move	df58b59fae750c4e7a6f325e12bc9c054b1ca6fd
PCL3	sui/svalue/with_verification/client_example/sources/push_client.move	ad3f72b410a488a34852ac2a2e19ad6d7fe01de1
MOV18	sui/svalue/with_verification/supra-svalue-feed-framework/Move.toml	aa48887e204eeebb3f96ce868eab503927eb4bc3
PDPV24	sui/svalue/with_verification/supra-svalue-feed-framework/sources/price_data_pull_v2.move	62da4aa2fd233232b3d9418760e12e3fb482690a
SFH3	sui/svalue/with_verification/decentralized_im/supra_holder/sources/svalue_feed_holder.move	598a11961f6ad9f76b865c07f1237264fb11d059
PDPV25	sui/svalue/with_verification/decentralized_im/supra_holder/sources/price_data_pull_v2.move	01aa778aa1a646bf80a48475c70675f5ddb3b740
VV23	sui/svalue/with_verification/decentralized_im/supra_validator/sources/validator_v2.move	152072d258d5e56ff38692e2b7db79ee72508320
VAL3	sui/svalue/with_verification/decentralized_im/supra_validator/sources/validator.move	b039a68b03082915c0c988bdcb8ac0eed935ff90

EMA1	sui/svalue/with_verification/decentralized_im/supra_utils/sources/enumerable_map.move	4613b4fa020a87a65350c91ce00a8246642eac30
UTI3	sui/svalue/with_verification/decentralized_im/supra_utils/sources/utils.move	850f45488e228ea2055a615dd6132303d0ce65c1

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	2	2	0
Informational	1	1	0
Minor	1	1	0
Medium	0	0	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 Supra to identify any potential issues and vulnerabilities in the source code of the Supra V2 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 2 issues of varying severity, listed below.

ID	Title	Severity	Status
PDP-1	Centralization Risk	Minor	Fixed
VV2-1	`EINVALID_LENGTH` Is Never Used	Informational	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the Supra V2 Smart Contract :

Multi-sig account

- `Multi-sig` can upgrade the package through `migrate` function.
- `Multi-sig` can add/updates the public key associated with the given `committee_id` in the `DkgState` through `add_committee_public_key` function.
- `Multi-sig` can remove the public key associated with the given `committee_id` in the `DkgState` through `remove_committee_public_key` function.

4 Findings

PDP-1 Centralization Risk

Severity: Minor

Status: Fixed

Code Location:

move/svalue/with_verification/framework/supra_holder/sources/price_data_pull_v2.move;

sui/svalue/with_verification/decentralized/sources/price_data_pull_v2.move

Descriptions:

Centralization risk was identified in the smart contract.

In the contract, `owner` can perform some privileged functions like `clean_up_old_root_hashes` which isn't used anywhere but can disable all the old `roothash` with arbitrary timestamps.

Suggestion:

It is recommended that measures be taken to reduce the centralization issue like using multi-sig.

Resolution:

The client has fixed this issue by removing the `clean_up_old_root_hashes` function.

VV2-1 EINVALID_LENGTH Is Never Used

Severity: Informational

Status: Fixed

Code Location:

move/svalue/with_verification/framework/supra_validator/sources/validator_v2.move#16

Descriptions:

In the validator_v2 contract, the error code EINVALID_LENGTH is never used.

Suggestion:

It is suggested to consider the related condition or remove the unnecessary error code.

Resolution:

The client has fixed this issue by removing the unused error code.

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.

MOVEBIT VERIFIED

MOVEBIT