SALUS SECURITY

APR 2024

CODE SECURITY ASSESSMENT

AVALON FINANCE

Overview

Project Summary

- Name: Avalon Finance - ORACLE
- Platform: Merlin
- Language: Solidity
- Repository:
  - https://github.com/avalonfinancexyz/ORACLE
  - https://github.com/avalonfinancexyz/Avalon
- Audit Range: See Appendix - 1

Project Dashboard

Application Summary

Name	Avalon Finance - ORACLE
Version	v3
Type	Solidity
Dates	Apr 09 2024
Logs	Apr 07 2024; Apr 08 2024; Apr 09 2024

Vulnerability Summary

Total High-Severity issues	0
Total Medium-Severity issues	1
Total Low-Severity issues	2
Total informational issues	2
Total	5

Contact

E-mail: support@salusec.io

Risk Level Description

High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for clients' reputations or serious financial implications for clients and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental to the client's reputation if exploited, or is reasonably likely to lead to a moderate financial impact.
Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
Informational	The issue does not pose an immediate risk, but is relevant to security best practices or defense in depth.

Content

Introduction

1.1 About SALUS

At Salus Security, we are in the business of trust.

We are dedicated to tackling the toughest security challenges facing the industry today. By building foundational trust in technology and infrastructure through security, we help clients to lead their respective industries and unlock their full Web3 potential.

Our team of security experts employ industry-leading proof-of-concept (PoC) methodology for demonstrating smart contract vulnerabilities, coupled with advanced red teaming capabilities and a stereoscopic vulnerability detection service, to deliver comprehensive security assessments that allow clients to stay ahead of the curve.

In addition to smart contract audits and red teaming, our Rapid Detection Service for smart contracts aims to make security accessible to all. This high calibre, yet cost-efficient, security tool has been designed to support a wide range of business needs including investment due diligence, security and code quality assessments, and code optimisation.

We are reachable on Telegram (https://t.me/salusec), Twitter (https://twitter.com/salus_sec), or Email (support@salusec.io).

1.2 Audit Breakdown

The objective was to evaluate the repository for security-related issues, code quality, and adherence to specifications and best practices. Possible issues we looked for included (but are not limited to):

- Risky external calls
- Integer overflow/underflow
- Transaction-ordering dependence
- Timestamp dependence
- Access control
- Call stack limits and mishandled exceptions
- Number rounding errors
- Centralization of power
- Logical oversights and denial of service
- Business logic specification
- Code clones, functionality duplication

1.3 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release and does not give any warranties on finding all possible security issues with the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues.

Findings

2.1 Summary of Findings

ID	Title	Severity	Category	Status
1	Stable rate mode borrowing should be disabled	Medium	Business Logic	Resolved
2	Incompatible getRoundData() function with Chainlink	Low	Business Logic	Acknowledged
3	Third-party dependencies	Low	Dependency	Acknowledged
4	Incompatible getAnswer() and getTimestamp() functions with Chainlink	Informational	Business Logic	Acknowledged
5	Use immutable to save gas	Informational	Gas Optimization	Acknowledged

2.2 Notable Findings

Significant flaws that impact system confidentiality, integrity, or availability are listed below.

1. Stable rate mode borrowing should be disabled

Severity: Medium	Category: Business Logic
Target: - StableDebtToken-Merlin	

Description

The AAVE protocol has disabled stable debt tokens because of an unpublished vulnerability. The proposal suggests that AAVE should stop minting new stable debt tokens in response to potential attack vectors.

Based on the real-time status of the contracts on the chain, Avalon does not disable stable debt tokens. This could make Avalon vulnerable to attacks.

Recommendation

Consider updating the mint() function according to the AAVE's patch.

```
function mint(
  address,
  address,
  uint256,
  uint256
) external virtual override onlyPool returns (bool, uint256, uint256) {
  revert('STABLE_BORROWING_DEPRECATED');
}
```

Status

This issue has been resolved by the team with commit bd6c7ff.

2. Incompatible getRoundData() function with Chainlink

Severity: Low	Category: Business Logic
Target: - contracts/PythAggregatorV3.sol	

Description

PythAggregatorV3 is a port of a Chainlink aggregator powered by Pyth Network feeds.

contracts/PythAggregatorV3.sol:L68-L89

```
function getRoundData(
    uint80 _roundId
)
    external
    view
    returns (
        uint80 roundId,
        int256 answer,
        uint256 startedAt,
        uint256 updatedAt,
        uint80 answeredInRound
    )
{
    PythStructs.Price memory price = pyth.getPriceUnsafe(priceId);
    return (
        _roundId,
        int256(price.price),
        price.publishTime,
        price.publishTime,
        _roundId
    );
}
```

In Chainlink, the getRoundData() function is expected to return the price of a particular round. But in the PythAggregatorV3 contract, this function gets the current price from Pyth.

This could have serious implications for projects that rely on the getRoundData() function, even resulting in lost assets.

Recommendation

Since Pyth does not support querying prices for a specific round, PythAggregatorV3 should not support this function.
It is recommended to revert directly in the getRoundData() function.

Status

This issue has been acknowledged by the team.

3. Third-party dependencies

Severity: Low	Category: Dependency
Target: - Avalon protocol	

Description

The Avalon protocol relies on the AAVE protocol to enable the main business logic. The current audit treats third-party entities as black boxes and assumes they are working correctly. However, in reality, third parties could be compromised, resulting in the loss of user assets.

Recommendation

We understand that the business logic requires interaction with third parties. We encourage the team to regularly monitor the statuses of third parties to reduce the impacts when they are not functioning properly.

Status

This issue has been acknowledged by the team.

2.3 Informational Findings

4. Incompatible getAnswer() and getTimestamp() functions with Chainlink

Severity: Informational	Category: Business Logic
Target: - contracts/PythAggregatorV3.sol	

Description

In the previous version, the getAnswer() and getTimestamp() functions are used to query for a specific round. But in the PythAggregatorV3 contract, they return the latest results.

contracts/PythAggregatorV3.sol:L60-L66

```
function getAnswer(uint256) public view returns (int256) {
        return latestAnswer();
}

function getTimestamp(uint256) external view returns (uint256) {
        return latestTimestamp();
}
```

Recommendation

Consider reverting directly in the getAnswer() and getTimestamp() functions or removing them since they are deprecated according to Chainlink's documentation.

Status

This issue has been acknowledged by the team.

5. Use immutable to save gas

Severity: Informational	Category: Gas Optimization
Target: - contracts/PythUpdater.sol - contracts/PythAggregatorV3.sol	

Description

To reduce gas costs, the below state variables could be declared as immutable since their value is fixed after the contract has been deployed.

contracts/PythAggregatorV3.sol:L13-L14

```
bytes32 public priceId;
IPyth public pyth;
```

contracts/PythUpdater.sol:L7-L8

```
IPyth public pyth;
address public owner;
```

Recommendation

Consider adding the immutable modifier to the above-mentioned state variables.

Status

This issue has been acknowledged by the team.

Appendix

Appendix 1 - Files in Scope

This audit covered the following files in commit 71cf514 of the ORACLE repo:

File	SHA-1 hash
contracts/PythUpdater.sol	8b603307b28e5e9413c267542de206bd077c229b
contracts/PythAggregatorV3.sol	94cc29f06c50f81204bdcfec9769878c39930b29

and the following files in commit bb0fec4 of the Avalon repo, **which has the same deployment script as AAVE**:

File	SHA-1 hash
hardhat.config.ts	3a54db05688a421e818baf56d34b63c87e2b60d6
package.json	8bd59f7aa90ff9adc1b5d3b3fc6842aadbfbcb18
deploy/00-before-deploy.ts	d5b38d0609d9522ed265371e902db3ed41299d2f
deploy/01-after-deploy.ts	17c5335af4b12778d70d12ad8d4885e90850fb21
deploy/00_core/00_markets_registry.ts	905571e53f29be8f913bb06fcc1d8c6c184f3375
deploy/00_core/01_logic_libraries.ts	af7d10c28c6e18a76f42563bcd9e7d086e2db92e
deploy/01_periphery_pre/01_treasury.ts	26c0b84b961d25e7721c5f7063305d61ee3b1772
deploy/02_market/00_setup_addresses_provider.ts	366a1cbc0cbb9ea6e52f9420be792970a390e0ea
deploy/02_market/01a_pool_implementation.ts	5d2eed58be03c7571183943d5f6364787a76f94c
deploy/02_market/01b_l2_pool_implementation.ts	9eda51ddacd057c3699809af983447eb1cad336c
deploy/02_market/02_pool_configurator.ts	6ca3a1fb396702cea03d8545164549ff92aa15e8
deploy/02_market/03_init_acl.ts	c643def229e259d6520a3a8c7aafec39d8c989ee
deploy/02_market/04_deploy_oracles.ts	2b84dc3cec27a95794e5bff35758e262a376fc08
deploy/02_market/05_init_oracles.ts	726fdc607ff8bbea49a4529bc98407bee522ddf4
deploy/02_market/06_init_pool.ts	2922545866d9ee8be2a87b190351239b32d4bf8a
deploy/02_market/07_incentives.ts	9fc6ac79d71b6eca12afd8b2e2efbc2b82d4cb8e
deploy/02_market/08_tokens_implementations.ts	8006ae58d8fac9e2a47e34529a09131525971ed2
deploy/02_market/09_init_reserves.ts	76d91cb1f40deae707e61294a603b31b41782c3c

deploy/02_market/10_init_periphery.ts	d6cf5737fd5ab6eb75eec350c5a0b8f56de4fb48
deploy/03_periphery_post/01_native_token_gateway.ts	a21f8d01317c2e7e70e22f862be70a2d91dea1b3
deploy/03_periphery_post/02_wallet_balance_provider.ts	fe9beeb4cc886360eed3a7fe3b518c13180c1a12
deploy/03_periphery_post/03-ui-helpers.ts	553b15cd2f82ad9f8289c93a3972fa3fb6800a3d
deploy/03_periphery_post/04_paraswap_adapters.ts	f5ad2429bedb9a4ddde43946dbe2e66b95c86116
helpers/constants.ts	bd9cf88b0d5d7a0a7095a7d9219395a06d13020b
helpers/contract-deployments.ts	5981a6ab096d7dbd27315843f4247767dab5eb55
helpers/contract-getters.ts	276cbb9277ed7ab79d70536eb8d42d01f4001e0d
helpers/deploy-ids.ts	dbf44f35f457edff6f45845ab8f67d39eef25e06
helpers/env.ts	50314b0d3b54c4423eabefbd4205ff33f52ed3f4
helpers/hardhat-config-helpers.ts	55b4777d09b05c79be2bdd9fdeb18aafe7be03d0
helpers/index.ts	8d870e8037da4436a3c423dc504b53588184f540
helpers/init-helpers.ts	23e96437147231305b3762a4b4db82071d90e62d
helpers/market-config-helpers.ts	8c224b9603ca849913a9368ca1d222fed1fbf12c
helpers/types.ts	257174959429bb26965fd948bb3ab7dbd16b4d62
helpers/utilities/defender.ts	5b4fb55db24aa43ffec374f7b438472eca2189e1
helpers/utilities/fork.ts	6ec990229ee7d0a8a29d057197f223217654ea53
helpers/utilities/signer.ts	a6ae768654561a8379f5406407b8e832f7a54644
helpers/utilities/tx.ts	d1f4efca0fb25b5c7a586996be137331c87bb494
helpers/utilities/utils.ts	5ad434b829f4377819c5924f790eb579f004a1d9
markets/merlin/index.ts	d82c029df8834bc685b05fbdd6ae7eac6b084d4d
markets/merlin/rateStrategies.ts	5d3d14989807225c7a2b1080b3c92648c1afdc16
markets/merlin/reservesConfigs.ts	3ab50ac9f82f07feb7e141cd76dc999c1e9d395f
markets/merlinInn/index.ts	085a1f1c6d4dabeba8083c7ebe24c0ed6a8c7a7c
markets/merlinInn/rateStrategies.ts	5d3d14989807225c7a2b1080b3c92648c1afdc16
markets/merlinInn/reservesConfigs.ts	9ea70e69e4cfbb0f6ae5f7bef5541910508fd19b
scripts/deploy.full.main.config.js	40586eaee619d1afab4d790f93001af052bf0298
tasks/market-registry/market-registry-add.ts	02b0ecbef35b84b0e2ecb187aa74213438b2af94

tasks/misc/add-new-asset.ts	bc0b78b89967b1787fc0f1b1c423d19818b43a39
tasks/misc/deploy-paraswapAdapters.ts	d06e639be14adbc70548093835df693e779b8e05
tasks/misc/deploy-ui-helpers.ts	4843cd2ea660d91a5ec6cfaa8d4256016e67ab5c
tasks/misc/deploy-UiIncentiveDataProvider.ts	c140a2b0c2c1268fdfeba07b56d18f1a162a5c0e
tasks/misc/deploy-UiPoolDataProvider.ts	58e9fc45d82206180faf751ed37b68b909a738af
tasks/misc/disable-faucet-native-testnets.ts	2bd9f156cf25f8f5226fb61b1904f4b32ec2d60b
tasks/misc/faucet.ts	aba9a3cf89189e2a112a5f5b47eb8be5dc4fb11a
tasks/misc/print-deployments.ts	9eb8659d79088a6244f376a2403323ebdd2c114b
tasks/misc/renounce-pool-admin.ts	1fc51f65892f815c64b2b660d1696a49526c9563
tasks/misc/review-atokens.ts	4c661d19c27bec68ca1c6083c35e4854e2868c72
tasks/misc/review-e-mode.ts	7f3d52aceaef72dad9ad6824269ba80984dedcf1
tasks/misc/review-rate-strategies.ts	600457296f4ae24aa12945d118dbaa9842b7e205
tasks/misc/review-stable-borrow.ts	6c8c7a7e07086e6ede98aba7da2d03753210d7a6
tasks/misc/review-supply-caps.ts	25dba4e773e109505325946a399764d60a8cabc8
tasks/misc/set-fallback-oracle.ts	b8cc346d3bcc83a0019236339aa7251716eb025d
tasks/misc/set-oracle.ts	7e96e722c24bca2e3c9328fb0bf8afd9cba115fe
tasks/misc/setup-debt-ceiling.ts	f4b1f10da2b70db341607e6e1379f99da23c79df
tasks/misc/setup-e-modes.ts	7cab4c074c255554a7ea43b691d13a448dc37c19
tasks/misc/setup-isolation-mode.ts	24ecd2b5a42a72d7b9fc15d48c2de2232e3cb37a
tasks/misc/setup-liquidation-protocol-fee.ts	eec399af5fc60356c78add745c51607f1952a2af
tasks/misc/setup-rewards-incentives.ts	3293178338a8beaaed2c75f62bc035811146ad4f
tasks/misc/transfer-ownership.ts	7a283ef5f85b9b2b4a9dd0f3e876bd5bc3339ca9
tasks/misc/transfer-protocol-ownership.ts	66ae30924a5f49df3f9fe3a154cb128544610ba3
tasks/misc/upgrade-atokens-and-review.ts	b2de0b849f33a909f5fb3f173e42150d1b2b62c8
tasks/misc/upgrade-atokens.ts	1cc3ce2ca1562b21c2279f4f5ffaafc1019b7dc3
tasks/misc/verify-core.ts	078d455d70ad99b43d88073441d0a5c131fd525c
tasks/misc/verify-market.ts	ea88585ccd6686dd5bdf75bb6db2076bf4ea32f0
tasks/misc/verify-periphery-post.ts	1d3c6669951bb59351c81e2e16e8471a2140301b
tasks/misc/verify-periphery.ts	369f3ad7e33b0792a4f9d96c47238fdfc0a0d15d

tasks/misc/verify-tokens.ts	ed48ecd8eaaeda1d9499728fb058b9f46b0c23a4
tasks/misc/view-protocol-roles.ts	02965a7b221093d289d31058b5c5a2ea5313c775