SMART CONTRACT AUDIT REPORT

for

Automata Multi-Prover AVS

Prepared By: Xiaomi Huang

PeckShield

April 11, 2024

Document Properties

Client	Automata
Title	Smart Contract Audit Report
Target	Automata Multi-Prover AVS
Version	1.0
Author	Xuxian Jiang
Auditors	Jason Shen, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	April 11, 2024	Xuxian Jiang	Final Release
1.0-rc	April 10, 2024	Xuxian Jiang	Release Candidate

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Xiaomi Huang
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction 4

1.1 About Automata Multi-Prover AVS . . . 4

1.2 About PeckShield . . . 5

1.3 Methodology . . . 5

1.4 Disclaimer . . . 7

2 Findings 9

2.1 Summary . . . 9

2.2 Key Findings . . . 10

3 Detailed Results 11

3.1 Improved Initialization Logic in MultiProverServiceManager . . . 11

3.2 Revisited updatedCommittee() Logic in MultiProverServiceManager . . . 12

3.3 Trust Issue Of Admin Keys . . . 13

4 Conclusion 15

References 16

1 Introduction

Given the opportunity to review the design document and related smart contract source code of the `Automata Multi-Prover AVS` protocol, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About Automata Multi-Prover AVS

`Automata Multi-Prover AVS` targets to build a robust and fortified prover system through the use of diverse decentralized `TEE provers`. The `TEE prover` represents a pivotal type of co-processor, prioritizing integrity, verifiability, and transparency. It stands out as an efficient and robust solution for verifiable computing, integrating seamlessly with both on-chain and off-chain components. By employing `Eigenlayer`'s restaking protocol, the multi-prover system's security is significantly reinforced. Concurrently, the provision of economic incentives boosts prover participation, thus advancing the system's decentralization. The basic information of audited contracts is as follows:

Table 1.1: Basic Information of Automata Multi-Prover AVS

Item	Description
Name	Automata Multi-Prover AVS
Type	EVM Smart Contract
Language	Solidity
Audit Method	Whitebox
Latest Audit Report	April 11, 2024

In the following, we show the Git repository of reviewed files and the commit hash values used in this audit. The repository contains a number of smart contracts and this audit only covers the contracts under the `contracts/src` directory.

- https://github.com/automata-network/multi-prover-avs.git (a9516ea)

And this is the commit ID after all fixes for the issues found in the audit have been checked in:

- https://github.com/automata-network/multi-prover-avs.git (68d6fe1)

1.2 About PeckShield

PeckShield Inc. [9] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [8]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the contract is considered safe regarding the check item. For any discovered issue, we might further deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.
- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.
- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.
- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [7], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings.

1.4 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 of 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. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 | Findings

2.1 Summary

Here is a summary of our findings after analyzing the `Automata Multi-Prover AVS` implementation. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logic, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	1	■
Low	2	■ ■
Informational	0	
Total	3	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities that need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 1 medium-severity vulnerability and 2 low-severity vulnerabilities.

Table 2.1: Key Automata Multi-Prover AVS Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Improved Initialization Logic in Multi-ProverServiceManager	Coding Practices	Resolved
PVE-002	Low	Revisited updatedCommittee() Logic in MultiProverServiceManager	Business Logic	Resolved
PVE-003	Medium	Trust Issue Of Admin Keys	Security Features	Mitigated

Beside the identified issues, we emphasize that for any user-facing applications and services, it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

3 | Detailed Results

3.1 Improved Initialization Logic in MultiProverServiceManager

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `MultiProverServiceManager`
- Category: Coding Practices [5]
- CWE subcategory: CWE-1126 [1]

Description

To facilitate possible future upgrade, the `MultiProverServiceManager` contract is instantiated as a proxy with actual logic contract in the backend. While examining the related contract construction and initialization logic, we notice current initialization can be improved.

In the following, we shows its constructor and initialization routines. We notice its constructor has properly invoked the following statement, i.e., `_disableInitializers()` (line 34). Note this statement is called in the logic contract where the initializer is locked. Therefore any user will not be able to call the `initialize()` function in the state of the logic contract and perform any malicious activity.

```
26      constructor(
27          IAVSDirectory __avsDirectory,
28          IRegistryCoordinator __registryCoordinator,
29          IStakeRegistry __stakeRegistry
30      )
31          BLSSignatureChecker(__registryCoordinator)
32          ServiceManagerBase(__avsDirectory, __registryCoordinator, __stakeRegistry)
33      {
34          _disableInitializers();
35      }

37      function initialize(
38          IPauserRegistry _pauserRegistry,
39          uint256 _initialPausedStatus,
40          address _initialOwner,
41          address _stateConfirmer,
```

```
42         bool _poaEnabled
43     ) public initializer {
44         _initializePauser(_pauserRegistry, _initialPausedStatus);
45         _transferOwnership(_initialOwner);
46         _setStateConfirmer(_stateConfirmer);
47         poaEnabled = _poaEnabled;
48     }
```

Listing 3.1: `MultiProverServiceManager::constructor()/initialize()`

It comes to our attention that the above `initialize()` routine can be improved by calling `__ServiceManagerBase_init(_initialOwner)` to replace current `_transferOwnership(_initialOwner)` (line 45). The reason is that the `MultiProverServiceManager` contract needs to invoke the initialization routine of its parent contracts, including `ServiceManagerBase`.

Recommendation Improve the above-mentioned initialization routine in the `MultiProverServiceManager` contract.

Status This issue has been fixed in the following commit: `501b1d8`.

3.2 Revisited updatedCommittee() Logic in MultiProverServiceManager

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `MultiProverServiceManager`
- Category: Business Logic [6]
- CWE subcategory: CWE-841 [3]

Description

The `Automata Multi-Prover AVS` protocol by design allows for flexible committee management. While reviewing this design, we notice current committee-updating implementation may be improved.

To elaborate, we show below the related `updateCommittee()` routine. As the name indicates, this routine can be used by `owner` to update the given committee. Note current logic ensures any new `teeQuorumNumber` in the given committee is valid. However, it does not remove the associated connection from the old `teeQuorumNumber`. In other words, an old `teeQuorumNumber` still has a valid mapping in the `quorumIdToCommitteeId` structure. To fix, we can simply remove all `teeQuorumNumbers` from the given committee before adding new `teeQuorumNumbers`.

```
    function updateCommittee(Committee memory committee) external onlyOwner {
        require(committees[committee.id].id != 0, "MultiProverServiceManager.
            updateCommittee: committee does not exist");
```

```
        for (uint256 i = 0; i < committee.teeQuorumNumbers.length; i++) {
            uint8 teeQuorumNumber = uint8(committee.teeQuorumNumbers[i]);
            require(teeQuorums[teeQuorumNumber].teeType != TEE.NONE, "
                MultiProverServiceManager.addCommittee: tee quorum does not exist");
            require(quorumIdToCommitteeId[teeQuorumNumber] == 0  quorumIdToCommitteeId[
                teeQuorumNumber] == committee.id, "MultiProverServiceManager.
                updateCommittee: tee quorum is used by another committee");
            quorumIdToCommitteeId[teeQuorumNumber] = committee.id;
        }

        committees[committee.id] = committee;
    }
```

Listing 3.2: `MultiProverServiceManager::updateCommittee()`

Recommendation Revisit the above routine to adjust the `committee`.

Status This issue has been fixed in the following commit: `501b1d8`.

3.3 Trust Issue Of Admin Keys

- ID: PVE-003
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `MultiProverServiceManager`
- Category: Security Features [4]
- CWE subcategory: CWE-287 [2]

Description

In the `Automata Multi-Prover AVS` protocol, there is a privileged `owner` account that plays a critical role in governing and regulating the protocol-wide operations (e.g., configure various system parameters, manage allow lists, and upgrade the contract). In the following, we show the representative functions potentially affected by the privilege of the `owner` account.

```
    function addTEEQuorum(TEEQuorum memory teeQuorum) external onlyOwner {
        require(teeQuorums[teeQuorum.quorumNumber].teeType == TEE.NONE, "
            MultiProverServiceManager.addTEEQuorum: tee quorum already exists");
        require(_stakeRegistry.getTotalStakeHistoryLength(teeQuorum.quorumNumber) != 0,
            "MultiProverServiceManager.addTEEQuorum: quorum not initialized");

        teeQuorums[teeQuorum.quorumNumber] = teeQuorum;}

    function removeTEEQuorum(uint8 quorumNumber) external onlyOwner {
        require(teeQuorums[quorumNumber].teeType != TEE.NONE, "MultiProverServiceManager
            .removeTEEQuorum: tee quorum does not exist");
        require(quorumIdToCommitteeId[quorumNumber] == 0, "MultiProverServiceManager.
            removeTEEQuorum: tee quorum is in use");

```

```
        delete teeQuorums[quorumNumber];}

    function setStateConfirmer(address _stateConfirmer) external onlyOwner {
        _setStateConfirmer(_stateConfirmer);}

    function enablePoA() external onlyOwner {
        require(!poaEnabled, "MultiProverServiceManager.enablePoA: PoA already enabled");
        poaEnabled = true;}

    function disablePoA() external onlyOwner {
        require(poaEnabled, "MultiProverServiceManager.disablePoA: PoA already disabled");
        poaEnabled = false;}

    function whitelistOperator(address operator) external onlyOwner {
        require(operator != address(0), "MultiProverServiceManager.whitelistOperator: operator cannot be the zero address");
        require(!operatorWhitelist.contains(operator), "MultiProverServiceManager.whitelistOperator: operator already whitelisted");
        operatorWhitelist.add(operator);}

    function blacklistOperator(address operator) external onlyOwner {
        require(operator != address(0), "MultiProverServiceManager.blacklistOperator: operator cannot be the zero address");
        require(operatorWhitelist.contains(operator), "MultiProverServiceManager.blacklistOperator: operator not whitelisted");
        operatorWhitelist.remove(operator);}
```

Listing 3.3: Privileged Operations in `MultiProverServiceManager`

Note that if the privileged `owner` account is a plain `EOA` account, this may be worrisome and pose counter-party risk to the protocol users. A multi-sig account could greatly alleviate this concern, though it is still far from perfect. Specifically, a better approach is to eliminate the administration key concern by transferring the role to a community-governed `DAO`. In the meantime, a timelock-based mechanism can also be considered as mitigation.

Recommendation Promptly transfer the privileged account to the intended `DAO`-like governance contract. All changed to privileged operations may need to be mediated with necessary timelocks. Eventually, activate the normal on-chain community-based governance life-cycle and ensure the intended trustless nature and high-quality distributed governance.

Status The issue has been confirmed and the team plans to mitigate it with a `multi-sig`.

4 Conclusion

In this audit, we have analyzed the design and implementation of the `Automata Multi-Prover AVS` protocol, which targets to build a robust and fortified prover system through the use of diverse decentralized `TEE provers`. The `TEE prover` represents a pivotal type of co-processor, prioritizing integrity, verifiability, and transparency. It stands out as an efficient and robust solution for verifiable computing, integrating seamlessly with both on-chain and off-chain components. By employing `Eigenlayer`'s restaking protocol, the multi-prover system's security is significantly reinforced. Concurrently, the provision of economic incentives boosts prover participation, thus advancing the system's decentralization. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

References

[1] MITRE. CWE-1126: Declaration of Variable with Unnecessarily Wide Scope. https://cwe.mitre.org/data/definitions/1126.html.

[2] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[3] MITRE. CWE-841: Improper Enforcement of Behavioral Workflow. https://cwe.mitre.org/data/definitions/841.html.

[4] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[5] MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

[6] MITRE. CWE CATEGORY: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.html.

[7] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[8] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[9] PeckShield. PeckShield Inc. https://www.peckshield.com.