



# SMART CONTRACT AUDIT REPORT

for

AltLayer Mach AVS



Prepared By: Xiaomi Huang

PeckShield  
April 7, 2024

## Document Properties

Client	AltLayer
Title	Smart Contract Audit Report
Target	AltLayer Mach 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 7, 2024	Xuxian Jiang	Final Release
1.0-rc	April 3, 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

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	About AltLayer Mach AVS . . . . .	4
1.2	About PeckShield . . . . .	5
1.3	Methodology . . . . .	5
1.4	Disclaimer . . . . .	7
<b>2</b>	<b>Findings</b>	<b>9</b>
2.1	Summary . . . . .	9
2.2	Key Findings . . . . .	10
<b>3</b>	<b>Detailed Results</b>	<b>11</b>
3.1	Improved Initialization Logic in MachServiceManager . . . . .	11
3.2	Trust Issue Of Admin Keys . . . . .	12
<b>4</b>	<b>Conclusion</b>	<b>15</b>
	<b>References</b>	<b>16</b>

# 1 | Introduction

Given the opportunity to review the design document and related smart contract source code of the AltLayer Mach 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 AltLayer Mach AVS

AltLayer Mach AVS is a fast finality layer for Ethereum rollups. In Mach AVS, operators will run verifier nodes for rollups, monitor the rollup for fraudulent behavior, and submit a fraudulent alert to Mach AVS. Fraudulent alert can then be confirmed via sufficient quorum or zk proofs. The basic information of audited contracts is as follows:

Table 1.1: Basic Information of AltLayer Mach AVS

Item	Description
Name	AltLayer Mach AVS
Type	EVM Smart Contract
Language	Solidity
Audit Method	Whitebox
Latest Audit Report	April 7, 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 `MachServiceManager.sol` contract.

- <https://github.com/alt-research/mach-avs.git> (87668b6)

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

- <https://github.com/alt-research/mach-avs.git> (6d02245)

## 1.2 About PeckShield

PeckShield Inc. [7] 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](mailto:contact@peckshield.com)).

Table 1.2: Vulnerability Severity Classification

Impact	High	Medium	Low
	Critical	High	Medium
	High	Medium	Low
	Medium	Low	Low
Likelihood			

## 1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [6]:

- 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.

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

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

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) [5], 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
<b>Configuration</b>	Weaknesses in this category are typically introduced during the configuration of the software.
<b>Data Processing Issues</b>	Weaknesses in this category are typically found in functionality that processes data.
<b>Numeric Errors</b>	Weaknesses in this category are related to improper calculation or conversion of numbers.
<b>Security Features</b>	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
<b>Time and State</b>	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.
<b>Error Conditions, Return Values, Status Codes</b>	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.
<b>Resource Management</b>	Weaknesses in this category are related to improper management of system resources.
<b>Behavioral Issues</b>	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
<b>Business Logics</b>	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.
<b>Initialization and Cleanup</b>	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
<b>Arguments and Parameters</b>	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
<b>Expression Issues</b>	Weaknesses in this category are related to incorrectly written expressions within code.
<b>Coding Practices</b>	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 `AltLayer Mach 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	1	
Informational	0	
Total	5	

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 1 low-severity vulnerability.

Table 2.1: Key AltLayer Mach AVS Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Improved Initialization Logic in MachServiceManager	Coding Practices	Resolved
PVE-002	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 MachServiceManager

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: MachServiceManager
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

#### Description

To facilitate possible future upgrade, the `MachServiceManager` token 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 initialization routine. We notice its constructor has properly invoked the following statement, i.e., `_disableInitializers()`. 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.

```
72     function initialize(  
73         IPauserRegistry _pauserRegistry,  
74         uint256 _initialPausedStatus,  
75         address _initialOwner,  
76         address _alertConfirmer  
77     ) public initializer {  
78         _initializePauser(_pauserRegistry, _initialPausedStatus);  
79         _transferOwnership(_initialOwner);  
80         _setAlertConfirmer(_alertConfirmer);  
81         allowlistEnabled = true;  
82         quorumThresholdPercentage = 66;  
83     }
```

Listing 3.1: `MachServiceManager::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 79). The reason is that the `MachServiceManager` contract needs to invoke the initialization routine of its parent contracts, including `ServiceManagerBase`.

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

**Status** This issue has been fixed in the following commit: `d006675`.

## 3.2 Trust Issue Of Admin Keys

- ID: PVE-002
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `MachServiceManager`
- Category: Security Features [3]
- CWE subcategory: CWE-287 [2]

### Description

In the AltLayer Mach 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.

```

93     function addToAllowlist(address operator) external onlyOwner {
94         if (operator == address(0)) {
95             revert ZeroAddress();
96         }
97         if (allowlist[operator]) {
98             revert AlreadyInAllowlist();
99         }
100        allowlist[operator] = true;
101        emit OperatorAllowed(operator);
102    }
103
104    /**
105     * @notice Remove an operator from the allowlist.
106     * @param operator The operator to remove
107     */
108    function removeFromAllowlist(address operator) external onlyOwner {
109        if (!allowlist[operator]) {
110            revert NotInAllowlist();
111        }
112        allowlist[operator] = false;
113        emit OperatorDisallowed(operator);

```

```

114     }
115
116     /**
117      * @notice Enable the allowlist.
118      */
119     function enableAllowlist() external onlyOwner {
120         allowlistEnabled = true;
121         emit AllowlistEnabled();
122     }
123
124     /**
125      * @notice Disable the allowlist.
126      */
127     function disableAllowlist() external onlyOwner {
128         allowlistEnabled = false;
129         emit AllowlistDisabled();
130     }
131
132     /**
133      * @notice Remove an Alert.
134      * @param messageHash The message hash of the alert
135      */
136     function removeAlert(bytes32 messageHash) external onlyOwner {
137         _messageHashes.remove(messageHash);
138         emit AlertRemoved(messageHash, _msgSender());
139     }
140
141     /**
142      * @notice Update quorum threshold percentage
143      * @param thresholdPercentage The new quorum threshold percentage
144      */
145     function updateQuorumThresholdPercentage(uint8 thresholdPercentage) external
146         onlyOwner {
147         quorumThresholdPercentage = thresholdPercentage;
148         emit QuorumThresholdPercentageChanged(thresholdPercentage);
149     }

```

Listing 3.2: Privileged Operations in `MachServiceManager`

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 AltLayer Mach AVS protocol, which is a fast finality layer for Ethereum rollups. In Mach AVS, operators will run verifier nodes for rollups, monitor the rollup for fraudulent behavior, and submit a fraudulent alert to Mach AVS. Fraudulent alert can then be confirmed via sufficient quorum or zk proofs. 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 CATEGORY: 7PK - Security Features. <https://cwe.mitre.org/data/definitions/254.html>.
- [4] MITRE. CWE CATEGORY: Bad Coding Practices. <https://cwe.mitre.org/data/definitions/1006.html>.
- [5] MITRE. CWE VIEW: Development Concepts. <https://cwe.mitre.org/data/definitions/699.html>.
- [6] OWASP. Risk Rating Methodology. [https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology).
- [7] PeckShield. PeckShield Inc. <https://www.peckshield.com>.