# SERPA

## AllmarsGovernor Smart Contract Audit

If you have any questions about smart-contract audit, contact us hello@serpa.software

29.10.2022 www.serpa.software

# TABLE OF CONTENTS

**INTRODUCTION** 3
**AUDIT METHODOLOGY** 4
Design Patterns 4
Static Analysis 4
Security Issues Analysis 4
Manual Analysis 5
Contracts Reviewed 6
**AUDIT SUMMARY** 7
Analysis Results 7
Test Results 7
**ISSUES DISCOVERED** 8
Severity Levels 8
Issues 8
Informational 8
**CONCLUSION** 9

# INTRODUCTION

Our company provides comprehensive, independent smart contract auditing. We help stakeholders confirm the quality and security of their smart contracts using our standardized audit process. The scope of this audit was to analyze and document the AllmarsGovernor contract (deployed to the Polygon mainnet at the 29-th of October 2022 at 0xA2C14Ab02ee48E85E73d36eE20456c2CbdF8E047).

# AUDIT METHODOLOGY

AllmarsGovernor contracts audit consist of four categories of analysis.

**1. Design Patterns**

We inspect the structure of the smart contract, including both manual and automated analysis.

Contract that was written by developers is not well commented (comments are missed for most custom functions of the contract).

Code is not unified (using of lead underscore and upper case for variables and constants names doesn’t correlate with type and visibility).

**2. Static Analysis**

The static analysis is performed using a series of automated tools, purposefully designed to test the security of the contract.

All the issues found by tools were manually checked (rejected or confirmed).

**3. Security Issues Analysis**

Contract reviewing to identify common vulnerabilities.

- Re-Entrancy, a critical flaw where one contract exploits the execution state of another contract. Overall Severity: Critical

Not found.

- Self-Destructing Contract, a flaw in how a library contract delegates its functions to smart contracts that invoke it. Overall Severity: Critical

Not found.

- Transaction-Ordering Dependence, an uncommon flaw that allows a miner to manipulate a transaction's output by its timestamp. Overall Severity: Low

Not found.

- Timestamp Dependency, a bug that changes the result of a transaction depending on when it executes within a block. Overall Severity: Medium

Not found.

Contract time management cannot be affected in a critical way by possible 10-15 minutes timestamp manipulations.

- Assertion Failure, an indication that another, potentially critical flaw occurred upstream. Overall Severity: Medium

Not found.

**4. Manual Analysis**

Comparing of requirements and implementation. Reviewing of a smart contract for compliance with specified customer requirements. Checking for a gas optimization and self-documentation. Running tests of the properties of the smart contract in test net.

## 6. Contracts Reviewed

On October 29, 2022 following smart contract was reviewed:

Contract name: AllmarsGovernor
Compiler version 0.8.0, overall 2480 lines of code.

# AUDIT SUMMARY

The contract has been found to be free of security issues.

Contract has well-formed structure. Gas usage is optimal.

| Category of analysis | Result |
|---|---|
| Design Patterns | Updates Recommended |
| Security Issues Analysis | Passed |
| Static Analysis | Passed |
| Manual Analysis | Passed |

**Test Results.**

All tests run successfully with excellent code coverage.

# ISSUES DISCOVERED

Issues are listed from most critical to least critical. Severity is determined by an assessment of the risk of exploitation or otherwise unsafe behavior.

Severity Levels

- Informational - No impact on the contract.
- Low - Minimal impact on operational ability.
- Medium - Affects the ability of the contract to operate.
- High - Affects the ability of the contract to work as designed in a significant way.
- Critical - Funds may be allocated incorrectly, lost or otherwise result in a significant loss.

**Issues.**

1. Informational: There are not enough comments in the code.
   Recommended: Add comments to the contract functions.
2. Informational: Code is not unified.
   Recommended: Adjust constants and variables names according to the best practices.

## CONCLUSION

The AllmarsGovernor smart contract is well crafted, following common security practices. Full set of tests were provided to enforce correctness.