

Security Assessment

Aurus

Minter.sol

Smart Contracts Audit

Date: 9th October, 2022





Table of Content

Table of Content	2
Introduction	3
Auditing Approach and Methodologies	3
Audit Details	3
Audit Goals	4
Security	4
Sound Architecture	4
Code Correctness and Quality	4
Security	5
High-level severity issues	5
Medium level severity issues	5
Low-level severity issues	5
Informational-level severity issues	5
Vulnerability Summary	6
Manual Audit	7
Automated Audit	8
Solhint Linting Violations	8
Slither	8
Mythril	10
Disclaimer	11
Summary	11



1. Introduction

This Audit Report mainly focuses on the overall security of **Minter.sol**. With this report, we have tried to ensure the reliability and correctness of their smart contract by a complete and rigorous assessment of their system's architecture and the smart contract codebase.

1.1 Auditing Approach and Methodologies

The NonceAudit team has performed rigorous analysis of the project starting with analyzing the code design patterns in which we reviewed the smart contract architecture to ensure it is well structured and safe use of third-party smart contracts and libraries.

Our team then performed a formal line-by-line inspection of the Smart Contract to find any potential issues like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks. In Automated Testing, we tested the Smart Contract with industry standard tools to identify vulnerabilities and security flaws.

The audit approach included:

- Analyzing the complexity of the code in-depth and detailed, manual review of the code, line-by-line.
- Analyzing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analyzing the security of the on-chain data.

1.2 Audit Details

Project Name : Aurus

ID: ARS

Git commit hash: d53acf618090c9692372581a24ed72f0a76ad740

Languages: Solidity (Smart contracts)

Platforms and Tools: Remix IDE, Solhint, VScode, Slither, Mythril



2. Audit Goals

The focus of the audit was to verify that the Smart Contract System is secure, resilient, and working according to the specifications. The audit activities can be grouped into the following three categories:

2.1. Security

Identifying security-related issues within each contract and the system of contract.

2.2. Sound Architecture

Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.

2.3. Code Correctness and Quality

A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Sections of code with high complexity

3. Security



Every issue in this report was assigned a severity level from the following:

High-level severity issues

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium level severity issues

Issues on this level could potentially bring problems and should eventually be fixed.

Low-level severity issues

Issues on this level are minor details and warnings that can remain unfixed but would be better fixed.

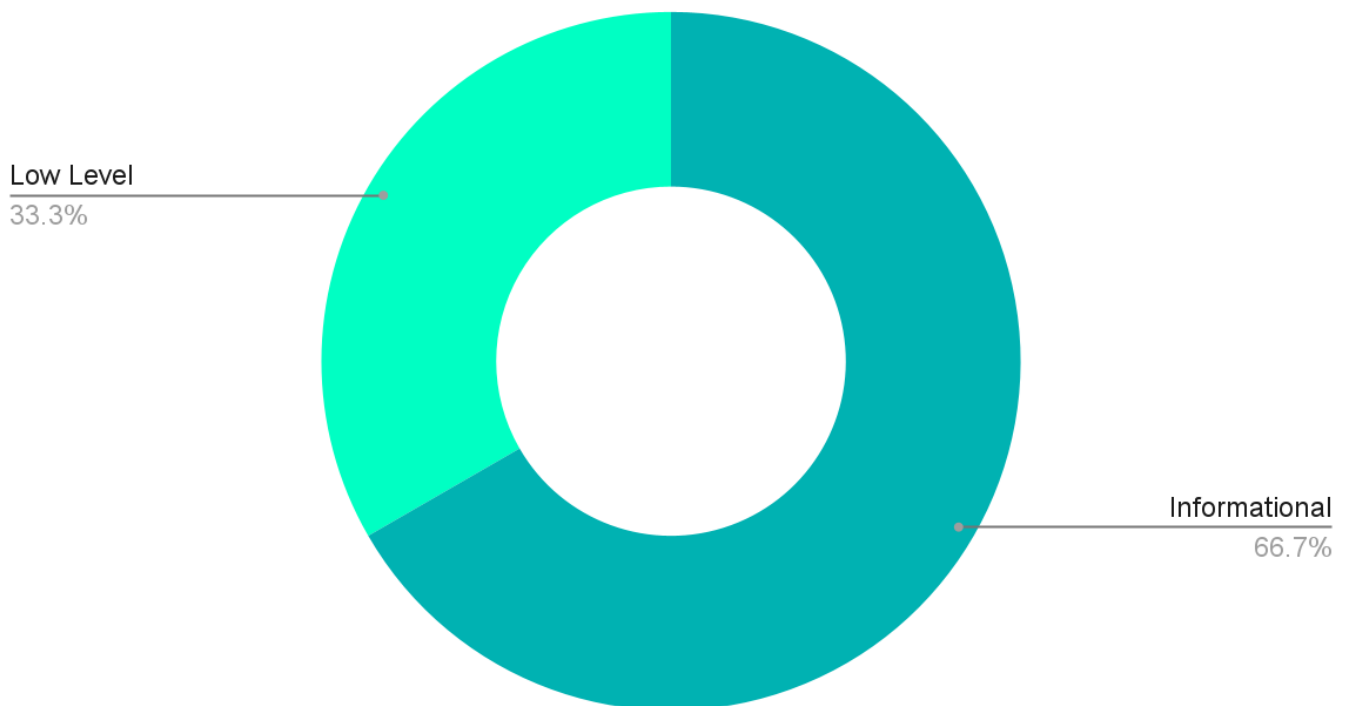
Informational-level severity issues

Issues on this level are informational details that can remain unfixed but would be better fixed.

4. Vulnerability Summary



Points scored



ID	Title	Severity	Status
ARS-01	Missing events arithmetic	Low level	CLOSED
ARS-02	Block timestamp	Low level	CLOSED
ARS-03	Incorrect versions of Solidity	Informational level	CLOSED
ARS-04	Unused state variable	Informational level	CLOSED
ARS-05	Public functions that could be declared external	Informational level	CLOSED
ARS-06	Missing SPDX License Identifier	Informational level	CLOSED



5. Manual Audit

For this section, the code was tested/read line by line by our developers. We also used Remix IDE's JavaScript VM to test the contract functionality.

- **High-level severity issues**

- Not Found

- **Medium level severity issues**

- Not Found

- **Low Level Severity issues**

- Not Found

- **Informational-level severity issues**

- **Title:** Missing SPDX License Identifier
- **ID:** ARS-06
- **Line of Code:** L1
- **status:** **CLOSED**
- **Description:** SPDX license identifier not provided in source file.
- **Recommendation:** Before publishing, consider adding a comment containing "SPDX-License-Identifier: <SPDX-License>" to each source file. Use "SPDX-License-Identifier: UNLICENSED" for non-open-source code.



6. Automated Audit

6.1 Solhint Linting Violations

Solhint is an open-source project for linting solidity code, providing both security and style guide validations. It integrates seamlessly into most mainstream IDEs. We used Solhint as a plugin within our Remix IDE for this analysis. Several violations were detected by Solhint, it is recommended to use [Solhint's npm package](#) to lint the contract.

```
13:5  warning  Variable name must be in mixedCase
14:5  warning  Variable name must be in mixedCase
23:9  warning  Error message for require is too long
96:30 warning  Avoid to make time-based decisions in your business logic
111:9 warning  Error message for require is too long
```

6.2 Slither

Slither, an open-source static analysis framework. This tool provides rich information about Ethereum smart contracts and has critical properties. While Slither is built as a security-oriented static analysis framework, it is also used to enhance the user's understanding of smart contracts, assist in code reviews, and detect missing optimizations.

- **High-level severity issues**

- Not Found

- **Medium level severity issues**

- Not Found

• Low Level Severity issues

- **Title:** Missing events arithmetic
 - **ID:** ARS-01
 - **Line of Code:** L37
 - **status:** CLOSED
 - **Description:** Detected missing events for critical arithmetic parameters. In `setMintingFee(uint256).`
 - **Recommendation:** Emit an event for critical parameter changes.
-

- **Title:** Block timestamp
- **ID:** ARS-02
- **Line of Code:** L84
- **status:** CLOSED
- **Description:** Dangerous usage of `block.timestamp`. `block.timestamp` can be manipulated by miners.
- **Recommendation:** Avoid relying on `block.timestamp`.

• Informational-level severity issues

- **Title:** Incorrect versions of Solidity
 - **ID:** ARS-03
 - **Line of Code:** L1
 - **status:** CLOSED
 - **Description:** `solc` frequently releases new compiler versions. Using an old version prevents access to new Solidity security checks. We also recommend avoiding complex `pragma` statements.
 - **Recommendation:** Deploy with any of the following Solidity versions:
 - 0.7.5 - 0.7.6
 - 0.8.4 - 0.8.7 Use a simple `pragma` version that allows any of these versions. Consider using the latest version of Solidity for testing.
-

- **Title:** Unused state variable
- **ID:** ARS-04
- **Line of Code:** L12
- **status:** CLOSED
- **Description:** `MAX_HEARTBEAT_DAYS` is declared but never used.
- **Recommendation:** Remove unused state variables.

- **Title:** Public functions that could be declared external
- **ID:** ARS-05
- **Line of Code:** L36 / L40 / L44 / L48 / L53 / L106
- **status:** CLOSED
- **Description:** public functions that are never called by the contract should be declared external to save gas.
- **Recommendation:** Use the external attribute for functions never called from the contract.

6.3 Mythril

Mythril is a security analysis tool for EVM bytecode. It detects security vulnerabilities in smart contracts built for Ethereum, Hedera, Quorum, Vechain, Roostock, Tron and other EVM-compatible blockchains. It uses symbolic execution, SMT solving and taint analysis to detect a variety of security vulnerabilities.

- **High-level severity issues**

- Not Found

- **Medium level severity issues**

- Not Found

- **Low Level Severity issues**

- Not Found

- **Informational-level severity issues**

- Not Found

7. Disclaimer

NonceAudit audit is not a security warranty, investment advice, or an endorsement of Aurus contract. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

8. Summary

The use case of the smart contract is simple and the code is relatively normal. Altogether, the code is written and demonstrates effective use of Ownable.



NonceAudits

www.nonceaudits.com