Throne Smart Contract Preliminary Audit Report

Project Synopsis

Project Name	**Throne**
Platform	Ethereum, Solidity
Github Repo	https://github.com/ThroneProject/ERC-20/blob/main/contracts/ThroneERC20.sol
Deployed Contract	Not Deployed
Total Duration	3 Days
Timeline of Audit	**1st September 2021 to 3rd September 2021**

Contract Details

Total Contract(s)	1
Name of Contract(s)	**`ThroneERC20`**
Language	Solidity
Commit Hash	***`21644bad95fb4023dd4c125f76b357c77d2b1446`***

Contract Vulnerabilities Synopsis

Issues	Open Issues	Closed Issues
Critical Severity	0	0
Medium Severity	0	0
Low Severity	2	0
Information	1	0
Total Found	3	0

Detailed Results

The contract has gone through several stages of the audit procedure that includes structural analysis, automated testing, manual code review, etc.

All the issues have been explained and discussed in detail below. Along with the explanation of the issue found during the audit, the recommended way to overcome the issue or improve the code quality has also been mentioned.

A. Contract Name: ThroneERC20

High Severity Issues

None Found

Medium Severity Issues

None Found

Low Severity Issues

A.1 External Visibility should be preferred

Explanation:

Functions that are never called throughout the contract should be marked as ***external*** visibility instead of ***public*** visibility.
This will effectively result in Gas Optimization as well.

Therefore, the following function must be marked as **external** within the contract:

- ***mint()*** *function at* ***Line 39***
- ***pause()*** *function at* ***Line 53***
- ***unpause()*** *function at* ***Line 67***

Recommendation:

If the **PUBLIC** visibility of the above-mentioned functions is not intended, then the **EXTERNAL** Visibility keyword should be preferred.

A.2 Invalid Error Messages found in Require Statements

Line no - 82, 98

Explanation:

The **ThroneERC20** contract includes a few require statements with misleading error messages in require statements.

The following functions, for instance, include error messages of ***Unpause*** while the functionality actually represents a ***Burn*** feature:

a. ***burn()*** *function at* ***Line 82***

b. ***burnFrom()*** *function at* ***Line 98***

```
76      /**
77       * @dev Destroys `amount` tokens from the caller.
78       *
79       * See {ERC20-_burn}.
80       */
81      function burn(uint256 amount) public override {
82          require(hasRole(OWNER_ROLE, _msgSender()), "ThroneERC20: must have owner role to unpause");
83          super.burn(amount);
84      }
85
```

While this badly affects the readability of the code, it also leads to a scenario where wrong information is provided to the user during a function revert.

Recommendation:

It is recommended to provide adequate error messages in require statement to avoid the above-mentioned scenarios.

Informational

A.3 Test cases can be improved

Explanation:

Test cases related to the access control and other imperative functionalities of the contract were not found in the current test files.

Recommendation:

It's recommended to write extensive test cases to ensure the contract executes as per expectation.

Automated Test Results

```
Compiled with solc
Number of lines: 1388 (+ 0 in dependencies, + 0 in tests)
Number of assembly lines: 0
Number of contracts: 16 (+ 0 in dependencies, + 0 tests)

Number of optimization issues: 15
Number of informational issues: 20
Number of low issues: 2
Number of medium issues: 4
Number of high issues: 0

ERCs: ERC165, ERC20

+---------------+-------------+-------------+--------------------+--------------+----------+
|      Name     | # functions |     ERCS    |     ERC20 info     | Complex code | Features |
+---------------+-------------+-------------+--------------------+--------------+----------+
|    Strings    |      4      |             |                    |     Yes      |          |
| EnumerableSet |      20     |             |                    |      No      |          |
|  ThroneERC20  |      70     | ERC20,ERC165 |      Pausable      |      No      |          |
|               |             |             |     ∞ Minting      |              |          |
|               |             |             | Approve Race Cond. |              |          |
|               |             |             |                    |              |          |
+---------------+-------------+-------------+--------------------+--------------+----------+
INFO:Slither:myFlat.sol analyzed (16 contracts)
```