NiftifyERC20 Smart Contract Final Audit Report

Project Synopsis

Project Name	**Niftify**
Platform	Ethereum, Solidity
Github Repo	https://github.com/Niftify-io/token-smart-contracts/blob/master/contracts/tokens/erc20/NiftifyERC20.sol
Deployed Contract	Not Deployed
Total Duration	4 Days
Timeline of Audit	**25th August to 30 August 2021**

Contract Details

Total Contract(s)	1
Name of Contract(s)	NiftifyERC20
Language	Solidity
Commit Hash	`19d63f7369e3b3c61a860ea147ac7bfb8c689ad7`

Contract Vulnerabilities Synopsis

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

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: NiftifyERC20.sol

High Severity Issues

None Found

Medium Severity Issues

None Found

Low Severity Issues

Informational

A.1 Inadequate Test Cases for NiftifyERC20 contract

Status: CLOSED

Explanation:

The test scripts for the NifitifyERC20.sol contract don't include the test cases for AccessControl procedures in the contract.

Recommendation:

Keeping in mind the immutable nature of Smart Contracts, it's always considered a better practice to include adequate test scripts related that covers every aspect of a function in the contract.

A.2 NatSpec Annotations must be included

Status: CLOSED

Description:

The smart contracts do not include the NatSpec annotations adequately.

Recommendation:

Cover by NatSpec all Contract methods.

Automated Test Results

```
Compiled with solc
Number of lines: 1552 (+ 0 in dependencies, + 0 in tests)
Number of assembly lines: 0
Number of contracts: 17 (+ 0 in dependencies, + 0 tests)

Number of optimization issues: 15
Number of informational issues: 27
Number of low issues: 5
Number of medium issues: 0
Number of high issues: 0

ERCs: ERC165, ERC20

+--------------+-------------+--------------+--------------------+--------------+-----------+
|     Name     | # functions |     ERCS     |     ERC20 info     | Complex code |  Features |
+--------------+-------------+--------------+--------------------+--------------+-----------+
|   Strings    |      4      |              |                    |     Yes      |           |
|    ECDSA     |      9      |              |                    |      No      | Ecrecover |
|              |             |              |                    |              |  Assembly |
|   Counters   |      4      |              |                    |      No      |           |
| NiftifyERC20 |      71     | ERC20,ERC165 |      Pausable      |      No      | Ecrecover |
|              |             |              |     No Minting     |              |  Assembly |
|              |             |              | Approve Race Cond. |              |           |
|              |             |              |                    |              |           |
+--------------+-------------+--------------+--------------------+--------------+-----------+
```

Test Cases

```
Pausable ERC20 Token
  ✓ allows to transfer when unpaused (53ms)
  ✓ allows to transfer when paused and then unpaused (59ms)
  ✓ reverts when trying to transfer when paused (150ms)
  ✓ Should be able to transfer with permit (147ms)
  transfer from
    ✓ allows to transfer from when unpaused
    ✓ allows to transfer when paused and then unpaused (43ms)
    ✓ reverts when trying to transfer from when paused
  Access control
    ✓ Admin should be able to assign operator role
    ✓ Operator should be able to pause/unpause contract
    ✓ Operator should not be able to assign roles (67ms)
    ✓ Admin should be able to revoke operator role
    ✓ Non operator should not be able to pause/unpause contract
    ✓ Admin should be able to assign/revoke admin role to anyone


13 passing (7s)
```