CYBERCOSMOUS

Together We Secure

SMA TOKEN SMART CONTRACT AUDIT REPORT

Date: 10-02-23
Platform: SMA Token
Language: Solidity

Disclaimer

THIS DOCUMENT MAY CONTAIN CONFIDENTIAL INFORMATION ABOUT IT SYSTEMS AND THE INTELLECTUAL PROPERTY OF THE CUSTOMER AS WELL AS INFORMATION ABOUT POTENTIAL VULNERABILITIES AND METHODS OF THEIR EXPLOITATION. THE REPORT CONTAINING CONFIDENTIAL INFORMATION CAN BE USED INTERNALLY BY THE CUSTOMER OR IT CAN BE DISCLOSED PUBLICLY AFTER ALL VULNERABILITIES ARE FIXED - UPON THE DECISION OF THE CUSTOMER.

Document

Name	Smart Contract Code Review and Security Analysis Report for SMA Token
Platform	Solidity
File 1	SWIM-Token.sol
MD5 hash	667ef46616063abe593b24ee677d9d83
SHA256 hash	8bd27567bd340c14a2b81e92d295c443427ca9f551e5c0a75ee633c27916473b
Date	10/02/2023

Audit Details

Audited Project	SMA Token
Deployer Address	0xAda756a0c650eADB38f0e06FB49c8062a7B402a4
Client Contacts	SWIM –Spreadwisdom contact@swimspreadwisdom.io
Blockchain	Ethereum-ETH
Project Website	https://www.swimspreadwisdom.io

Introduction

Cybercosmous (Auditor) was contracted by SWIM Spreadwisdom Team (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer`s smart contract and its code review conducted between 09/02/2023 – 10/02/2023.

This contract consist of 1 file.

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions are intended.
- Identify potential security issues with the smart contract.

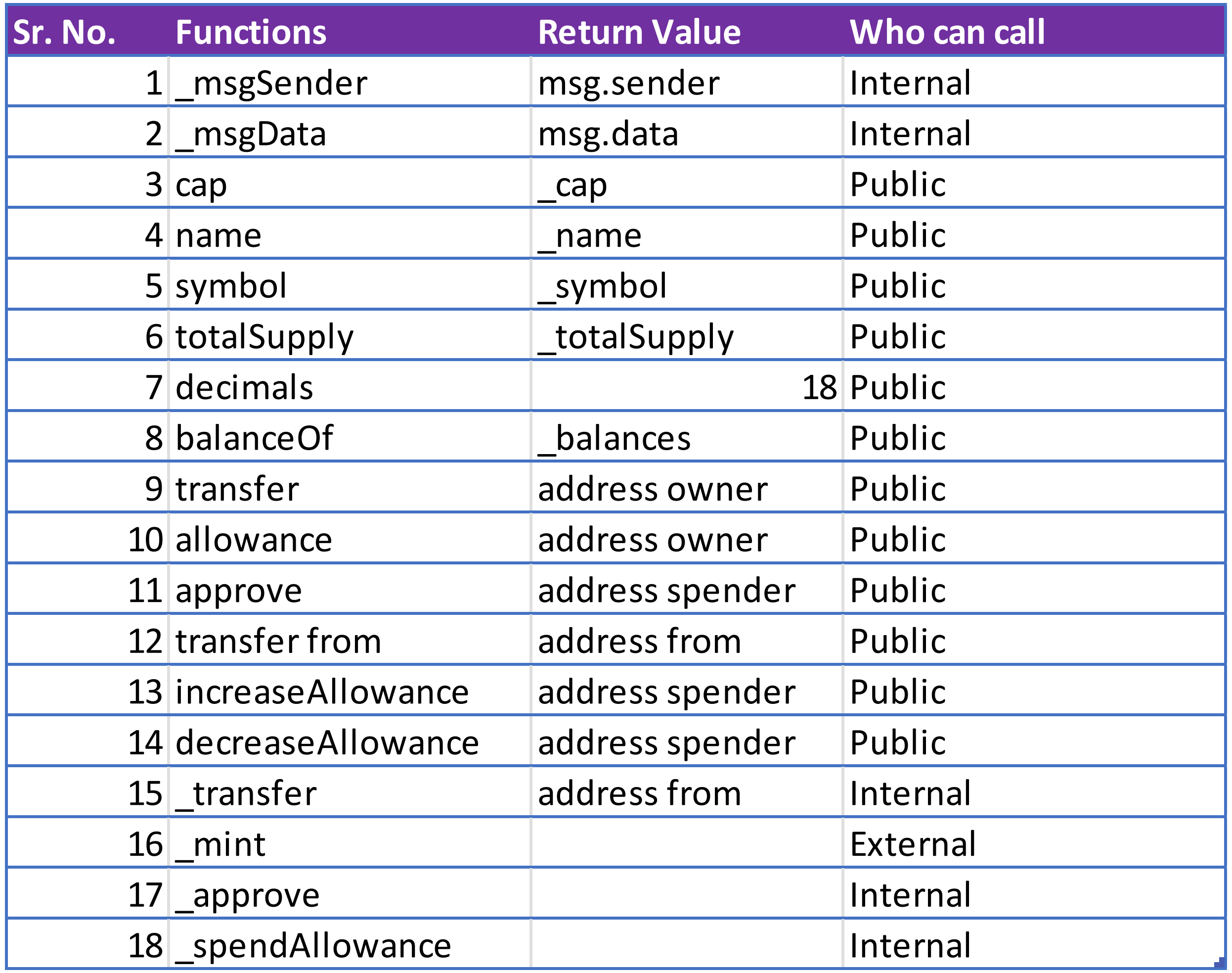
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improving the security posture of the smart contract by remediating the issues that were identified.

Project Scope

The scope of the project is a smart contract. We have scanned this smart contract for commonly known and more specific vulnerabilities, below are those considered (the full list includes but is not limited to):

- Reentrancy
- Timestamp Dependence
- Gas Limit & Loops
- DoS with (unexpected) Throw
- DoS with Block Gas Limit
- Transaction Ordering Dependence
- Byte array vulnerabilities
- Style guide vulnerabilities
- Transfer forwards all gas
- ERC20 Api violation
- Malicious Libraries
- Compiler version not fixed
- Unchecked external call – unchecked math
- Unsafe type interface
- Implicit visibility level
- Cross function race conditions

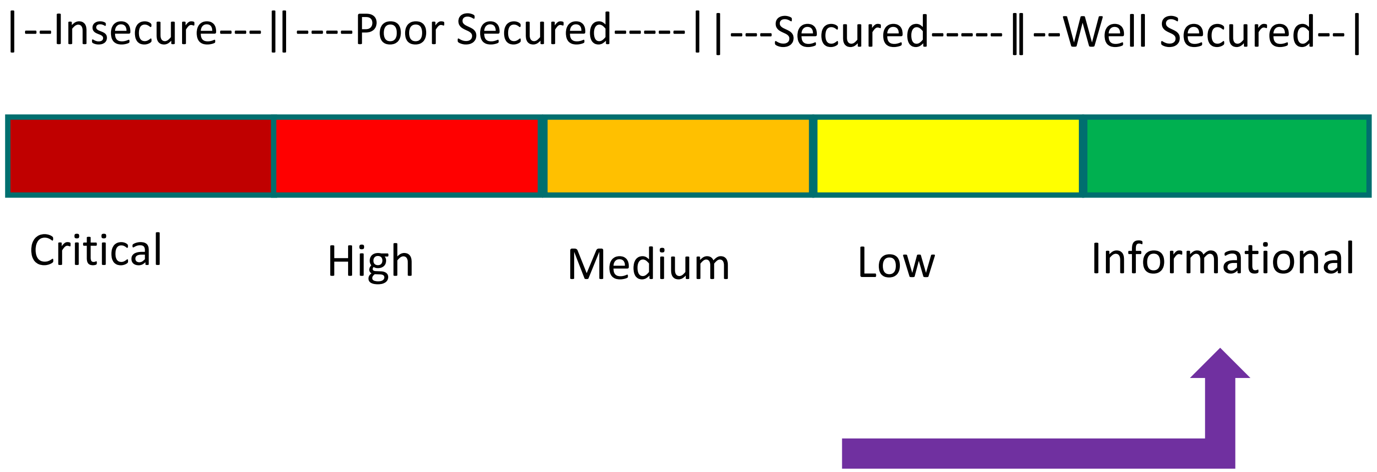
Contract Function Details



Sr. No.	Functions	Return Value	Who can call
1	_msgSender	msg.sender	Internal
2	_msgData	msg.data	Internal
3	cap	_cap	Public
4	name	_name	Public
5	symbol	_symbol	Public
6	totalSupply	_totalSupply	Public
7	decimals	18	Public
8	balanceOf	_balances	Public
9	transfer	address owner	Public
10	allowance	address owner	Public
11	approve	address spender	Public
12	transfer from	address from	Public
13	increaseAllowance	address spender	Public
14	decreaseAllowance	address spender	Public
15	_transfer	address from	Internal
16	_mint		External
17	_approve		Internal
18	_spendAllowance		Internal

Executive Summary

According to the assessment, the customer`s <Language of SMC> smart contract is well secured:



|--Insecure---||----Poor Secured-----||---Secured-----‖--Well Secured--|

Critical High Medium Low Informational

Manual & Automated checks are performed using industry standard tools and guidelines. All issues were checked and testing was performed by our team, which included the analysis of code functionality, manual testing of vulnerabilities found during automated analysis. The list of vulnerabilities found are mentioned further in the report.

Security Issues Test Status

Sr. No.	Security Issue Description	Test Status
1.	Compiler Errors	Passed
2.	Reentrancy	Passed
3.	Timestamp Dependencies	Passed
4.	Gas Limit & Loops	Passed
5.	DoS with (unexpected) Throw	Passed
6.	DoS with Block Gas Limit	Passed
7.	Transaction Ordering Dependence	Passed
8.	Byte array vulnerabilities	Passed
9.	Style guide vulnerabilities	Passed
10.	Transfer forwards all gas	Passed
11.	ERC20 API violation	Passed
12.	Unchecked external call – unchecked math	Passed
13.	Malicious Event Log	Passed
14.	Design Logic	Passed
15.	Cross function race conditions	Passed

Vulnerability Description

- **High Severity Issue**
  - No High severity issues found.

- **Medium Severity Issue**
  - No Medium severity issues found.

- **Low Severity Issue**
  1) No Low severity issues found

Conclusion

We were given a contract file. And we have used all possible tests based on the given object. The contract is written systematically but comments were missing.
We found no critical issues, So it is good to go for production.

Since possible test cases can be unlimited and developer level documentation (code flow diagram with function level description) not provided, for such extensive smart contract protocol, so we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Security state of reviewed contract is “ well secured ”.

Cybercosmous Auditor Disclaimer

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

Because the total number of test cases are unlimited, so the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug free status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only - we recommend proceeding with a detailed exhaustive testing of complete blockchain infrastructure assessment & a public bug bounty program to ensure security of smart contracts.

Technical Disclaimer

Smart contracts are deployed and executed on blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can’t guarantee explicit security of the audited smart contracts.

CYBERCOSMOUS

Together We Secure

Contact: chetaannt@vulhunt.in
Website: https://www.cybercosmous.com