Contract Audit Results

Prepared on: 7 Feb 2022

Contract: AUD445

Prepared by:

Charles Holtzkampf

Sentnlio Ltd

Prepared for:

Joe Rodgers

Viralcoin

Table of Contents

Executive Summary

This document outlines any issues found during the audit of the contracts:

- Viralcoin

  - The contract has **2** remarks.
  - **Owner privileges** (the ability of an owner to manipulate contract, may be risky for investors)
  - **No Major or Critical** security issues were found.
  - The risk associated with this contract is low, but investors should be aware that the owner has the ability to manipulate the contract.

REMARK	MINOR	MAJOR	CRITICAL
2	0	0	0

Severity Description

REMARK

Remarks are instances in the code that are worthy of attention, but in no way represent a security flaw in the code. These issues might cause problems with the user experience, confusion with new developers working on the project, or other inconveniences.

Things that would fall under remarks would include:

- Instances where best practices are not followed
- Spelling and grammar mistakes
- Inconsistencies in the code styling and structure

MINOR

Issues of Minor severity can cause problems in the code, but would not cause the code to crash unexpectedly or for funds to be lost. It might cause results that would be unexpected by users, or minor disruptions in operations. Minor problems are prone to become major problems if not addressed appropriately.

Things that would fall under minor would include:

- Logic flaws (excluding those that cause crashes or loss of funds)
- Code duplication
- Ambiguous code

MAJOR

Issues of major security can cause the code to crash unexpectedly, or lead to deadlock situations.

Things that would fall under major would include:

- Logic flaws that cause crashes
- Timeout exceptions
- Incorrect ABI file generation
- Unrestricted resource usage (for example, users can lock all RAM on contract)

CRITICAL

Critical issues cause a loss of funds or severely impact contract usage.

Things that would fall under critical would include:

- Missing checks for authorization
- Logic flaws that cause loss of funds
- Logic flaws that impact economics of system
- All known exploits (for example, on_notification fake transfer exploit)

Methodology

Throughout the review process, we check that the token contract:

- Documentation and code comments match logic and behaviour
- Is not affected by any known vulnerabilities

Our team follows best practices and industry-standard techniques to verify the proper implementation of the smart contract. Our smart contract developers reviewed the contract line by line, documenting any issues as they were discovered.

Our strategies consist largely of manual collaboration between multiple team members at each stage of the review, including:

I. Due diligence in assessing the overall code quality of the codebase.
II. Testing contract logic against common and uncommon attack vectors.
III. Thorough, manual review of the codebase, line-by-line.

Our testing includes

- Overflow Audit
- Authority Control Audit Authority Vulnerability Audit
- Authority Excessive Audit
- Safety Design Audit Hard-coded Audit
- Show coding Audit
- Abnormal check Audit
- Type safety Audit
- Denial of Service Audit
- Performance Optimization Audit
- Design Logic Audit
- False Notice Audit
- False Error Notification Audit

- Counterfeit Token Audit
- Random Number Security Audit
- Rollback Attack Audit

Audit Results –Viralcoin

REMARK - Owner privileges

Owner has the ability to mint and burn viral tokens, as well as update transfer fees (up to a maximum of 5%)

https://github.com/vcdcvcdc/viralcoin/blob/main/contracts/token/viral.sol

Suggested solution:

REMARK - Owner privileges

Contract owner is able to update vault information, including withdrawing of funds.

https://github.com/vcdcvcdc/viralcoin/blob/main/contracts/viralswap/ViralswapFactory.sol

Suggested solution:

Contract Files

Filename	SHA256
ViralswapERC20.sol	a966014e60566e51fbd2bd143a0bcc5b6970 8ab5aafc1e6a2dbefcaa5667df7d
ViralswapFactory.sol	118d2b758525bfb9f2d9ddd321ff7a2d6cc36 01a5ef9553473ff92acdcbdd8f8
ViralswapPair.sol	e1a5dd66b20567fed25bc79d0bba37385b9d a65c75c876f044e76a350182d66d
ViralswapRouter02.sol	c00126aa8971a15740d84ecf4af91ad25ebfb 813bc8065055cd10e3735293365
ViralswapVault.sol	a896cb2121f0759725c14ecba6ca712dc78b 005ac41caacfa8d0774646aa53eas
Math.sol	a553dd23aa798c18e1b2a19b2f64a2ba8144 df56e212f20bab346be5c37287bb
SafeMath.sol	7f35a13cbb97fa884bfa7bf32f1b1b84dea7a6 765825f511d3f732fbb8b7f435
TransferHelper.sol	28b7bb5e8ac8fb0a3ccdaf50b85d2dbc22804 d5b64d08f13924e94206ef823e1
UQ112x112.sol	24283a562d299a5e4133d3f05304eec8e75a 1b18c6907dd2a8f399eea0b16524
ViralswapLibrary.sol	3c323c7e495c8a79eccb70bfc836616a8238 3dfdca6365d4bdc6b1472051d3ad
viral.sol	2dc08676e6b7e191c263fb9c25dba20a0ee5 4f02609f402c775479eea64ec018