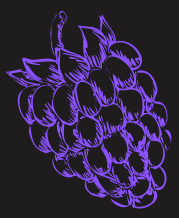


0XDAMORA
AUDITS

MARCH 2023

Vault Finance Audit

FOR

Vault Finance

PRESENTED BY

0xDaMora Warden

Table Of Contents:

1. Introduction

1.1 - Disclaimer 2

1.2 - Security Metodology 2

1.3 - Project Overview 4

1.4 - Project Dashbord 4

1.5 - Summary of Findings 5

1.6 - Conclusion 6

2. Finding Report

2.1 - Critical 7

2.2 - High 7

2.3 - Medium 7

2.4 - Low 8

3. About DaMora Audits 9

1. INTRODUCTION

1.1 - Disclaimer

The audit makes no statements or warranties about utility of the code, suitability of the business model, or any other statements about fitness of the contract to purpose, or their bug free status.
The audit documentation is for discussion purposes only.

1.2 - Security Metodology

The auditor is involved in the entire audit process, the code is reviewed and, if necessary, proof of concept is generated.
In case of detected vulnerabilities, the auditor works together with the project to solve them.

1- Proyect Review

- Proyect Documentation Review
- General Code Review
- Webpage Review

Goal:
Identify the business logic and purpose of the code to review.

2- Checking the Code

- Manual Code Cheking in search of more elaborate vulnerabilities.
- Automatic Code Checking using vulnerability analysis tools like Mythril, Slither, etc.

Goal:
Eliminate the possibility of the most typical vulnerabilities such as Reentrancy, flash loan, gas limits, overflow, underflow, etc.

3- Bug-Fixing and Re-Audit

- The client eliminates the vulnerabilities detected by the auditors
- The auditors proceed to make a new audit taking into account the arrangements implemented.

Goal:

A solution to the audit problems is generated and a final public audit is delivered.

Finding Severity Breakdown

All vulnerabilities discovered are clasiffied based on their potential severityand have the following classification:

Severity	Description
Critical	- Direct theft of any user funds, whether at-rest or in-motion, other than unclaimed yield - Direct theft of any user NFTs, whether at-rest or in-motion, other than unclaimed royalties - Permanent freezing of funds - Permanent freezing of NFTs - Unauthorized minting of NFTs - Protocol insolvency
High	- Theft of unclaimed yield - Theft of unclaimed royalties - Permanent freezing of unclaimed yield - Permanent freezing of unclaimed royalties - Temporary freezing of funds - Temporary freezing NFTs
Medium	- Smart contract unable to operate due to lack of token funds - Block stuffing for profit - Griefing (e.g. no profit motive for an attacker, but damage to the users or the protocol) - Theft of gas - Unbounded gas consumption
Low	- Contract fails to deliver promised returns, but doesn't lose value

1.3 - Proyect Overview

Vault Finance is a cryptocurrency that rewards its holders with daily BUSD payouts and offers a strategic buyback and burn wallet to help tokens appreciate in value. Additionally, eligible holders can receive additional tokens through the Diamond Hands Heist program. To protect investors, there is a maximum daily sell limit of 300 billion tokens per wallet.

1.4 - Proyect Dashboard

Project Summary and Scope

Title	**Description**
Vault Finance	daily BUSD payouts Token
Scope	**Link**
VFX Token(BSC)	https://bscscan.com/address/0xe06f46AFD251B06152B478d8eE3aCea534063994#code
DividendDistributor(BSC)	https://bscscan.com/address/0x1aa67e1b576ffc0ed12a224f84573c9011cb8841#code

1.5 - Summary of Findings

Automatic Tools:

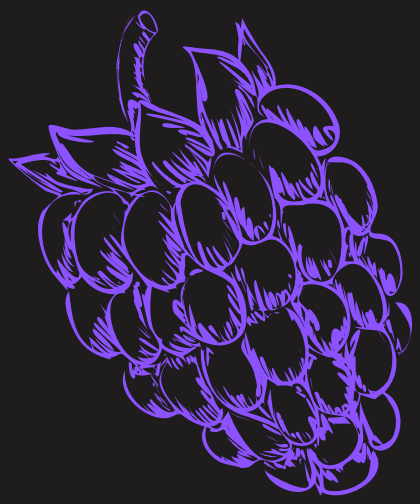
No	Description	Result
1	Compiler Warnings	Passed
2	Re-entrancy	Passed
3	Possible delays in data delivery	Passed
4	Front-running	Passed
5	Timestamp dependence	Passed
6	Integer Overflow and Underflow	Passed
7	DOS with Revert	Passed
8	DOS with block gas limit	Passed
9	Methods Execution permissions	Passed
10	Private User Data Leak	Passed
11	ShadowedStateVariable	Passed
12	UnrestrictedSelfdestruct	Passed
13	UnrestrictedDelegateCall	Passed

Manual Audit:

Severity	# of Findings
Critical	0
High	0
Medium	0
Low	2

1.6 - Conclusion

After conducting a thorough security audit of VFX Token platform, we are pleased to report that no major vulnerabilities were found. We found that Vault Finance have followed the best practices when deploying your contracts.



2. Finding Report

2.1 - Critical

Not Found

2.2 - High

Not Found

2.3 - Medium

Not Found

2.4 - Low

Low	Advanced Owner Privileges
File	VFX Token
Function	setExcludeFromDailyVolumeLimit setPoolsForExcludeFromDailyVolume
Severity	Low

Description:

It is possible for the owner to add users or pools that are excluded from the rule of number of tokens per day.

Recommendation:

Part of the appeal of Vault is the anti-dump security feature, it would be important to try not to use this feature too often.

2.4 - Low

Low	Owner Can BlackList Users.
File	VFX Token
Function	BlackList
Severity	Low

Description:

The owner has the privilege to deny the token transfer to any user.

Recommendation:

It can be a good security measure in the event of a FrontRunning attack, but should be used with justification and at the discretion of the Vault Finance owners.

Especial - Recomendation of Gas.

Gas	Distributor Optimized
File	DividendDistributor
Function	process(uint256)
Severity	High impact on efficiency

Description:

Process is in charge of distributing BUSD dividends to all users.

Recommendation:

It is possible to reduce up to 3000 gas per iteration, significantly increasing the efficiency in the distribution, instead of using a store each time iterating through currentIndex , the ideal is to allocate memory and store it at the end of all the iteration.

Ideally, since these are iterations that do not cause overflow, unchecked{} can be added to the currenindex in memory and to iterations, to reduce more gas.

3. About 0xDaMora Audits

0xDaMora is an emerging auditor who is starting to conduct code audits for Solidity.

By working with 0xDaMora, clients can benefit from a thorough examination of their Solidity code, including manual reviews, automated tests, and specialized tools to identify potential weaknesses.

CONTACTS:

@0xDaMora

danmor800@gmail.com

https://github.com/0xDaMora

0xDaMora#0655