## 

## 

NAME Audit



DATE

By Eat The Blocks

[**Introduction**](#_54qtnc3ppo6t) **3**

[Scope](#_c1m9k33qfiac) 3

[Analyses](#_3j2hvz6jg3l7) 3

[**Summary of Findings**](#_ccxge9kr1c9j) **4**

[Security Issues](#_4btsh2jjt0t9) 4

[**Security Issues Found**](#_gx01etlh80fx) **5**

[Severity Classification](#_cvxc58ui0u7g) 5

[Issues Status](#_af6jmuyxee7x) 5

[Critical Severity Issues](#_4bf6itpx7vak) 5

[CR-01 Issue Title (See Casing)](#_xm1nhvjsn8tb) 5

[Medium Severity Issues](#_4ovuqh4bbpck) 6

[Minor Severity Issues](#_n9ito55mu70h) 6

[**Enhancements**](#_u3o0vhrkvm70) **7**

[Table](#_w7c505unbodc) 7

[Details](#_3os5i0yzqbdr) 7

[EN-01 Description](#_xtebwhdsh84z) 7

[**Other Considerations**](#_yvrhfpu2kuvj) **7**

[Some Other Thing](#_n5smtkpv21go) 8

[**Changelog**](#_xq9np76lxnc9) **8**

# Introduction

EatTheBlocks was asked to audit the contracts for the XXXXX project. First, we will provide a summary of our discoveries and then we will show the details of our findings.

## Scope

The contracts audited are from the XXXXX git repository. The audit is based on the commit NNNNNNNN.

The audited contracts are:

* path/to/contract.sol: Description
* path/other: Description

The scope of the audit is limited to those files. No other files in this repository were audited. Its dependencies are assumed to work according to their documentation. Also, no tests were reviewed for this audit.

## Analyses

Without being limited to them, the audit process included the following analyses:

* Arithmetic errors
* Outdated version of Solidity compiler
* Race conditions
* Reentrancy attacks
* Misuse of block timestamps
* Denial of service attacks
* Excessive gas usage
* Missing or misused function qualifiers
* Needlessly complex code and contract interactions
* Poor or nonexistent error handling
* Insufficient validation of the input parameters
* Incorrect handling of cryptographic signatures
* Centralization and upgradeability

# Summary of Findings

We found N critical issues, M medium issues and several minor issues. Also, several enhancements were proposed.

All issues were fixed by the development team.

## Security Issues

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Title** | **Severity** | **Status** |
| CR-01 | Name | Critical | Resolved |
| ME-01 | Name | Medium | Mitigated |
| MI-01 | Name | Minor | Acknowledged |
| MI-02 | Name | Minor | Unresolved |
| MI-03 | Name | Minor | Partially Resolved |

# 

# Security Issues Found

## Severity Classification

Security risks are classified as follows:

* **Critical:** These are issues that we manage to exploit. They compromise the system seriously. They must be fixed **immediately**.
* **Medium:** These are potentially exploitable issues. Even though we did not manage to exploit them, or their impact is not clear, they might represent a security risk in the near future. We suggest fixing them **as soon as possible**.
* **Minor:** These issues represent problems that are relatively small or difficult to take advantage of but can be exploited in combination with other issues. These kinds of issues do not block deployments in production environments. They should be taken into account and be fixed **when possible**.

## Issues Status

An issue detected by this audit can have four distinct statuses:

* **Unresolved**: The issue has not been resolved.
* **Acknowledged**: The issue remains in the code but is a result of an intentional decision.
* **Resolved**: Adjusted program implementation to eliminate the risk.
* **Partially resolved**: Adjusted program implementation to eliminate part of the risk. The other part remains in the code but is a result of an intentional decision.
* **Mitigated**: Implemented actions to minimize the impact or likelihood of the risk.

## Critical Severity Issues

### CR-01 Issue Title (See Casing)

**Location**:

* contracts/contract1.sol:[NN-MM],
* contracts/contract2.sol:[NN]

Here goes some description explaining the problem and its impact and optionally some code. A Contract.function() may be mentioned or someVariable too. Also specific lines may be mentioned as Contract.sol in lines XX-YY.

Location is optional.

Fragments of solidity code are copy-pasted directly from VSCode with QuietLight Theme and then set to font-size 8 and remove space after paragraph (in Format -> Line & Paragraph Spacing). Like this:

*// Any yield should be paid out for the user*

uint256 amountVestedTokensWithYield = **IERC20**(token).**balanceOf**(address(this));

uint256 tokenGrantAmountToBeClaimed = tokenGrant.amount - tokenGrant.totalClaimed;

if(amountVestedTokensWithYield > tokenGrantAmountToBeClaimed) {

amountUserDeserve += (amountVestedTokensWithYield - tokenGrantAmountToBeClaimed);

}

if(!tokenGrant.initialClaimableCollected && (**currentTime**() > tokenGrant.startTime )) {

amountUserDeserve += tokenGrant.initiallyClaimableAmount;

}

tokenGrant.startTime = 0;

tokenGrant.amount = 0;

Recommendation

Generally, but not always, a recommendation on how to solve the issue is added. Take note that no heading style is used.

Status

**Unresolved|Acknowledged|Resolved|Mitigated**. After the dot, an optional description on how the issue was handled. For example: Fixed for commit xxxxxx. Will be Unresolved in the first delivery of the audit. Take note that no heading style is used.

## Medium Severity Issues

No issues found.

## Minor Severity Issues

No issues found.

# Enhancements

These items do not represent a security risk. They are best practices that we suggest implementing.

## Table

|  |  |  |
| --- | --- | --- |
| **ID** | **Title** | **Status** |
| EN-01 | Name | Not implemented |
| EN-02 | Name | Implemented |

## Details

### EN-01 Description

**Location**:

* contracts/contract1.sol:[NN-MM],
* contracts/contract2.sol:[NN]

Location is optional.

Recommendation

Generally, but not always, a recommendation on how to make the enhancement is added. Take note that no heading style is used.

Status

**Implemented|Not implemented**. After the dot, an optional description on how the proposal was handled.

# Other Considerations

The considerations stated in this section are not right or wrong. We do not suggest any action to fix them. But we consider that they may be of interest for other stakeholders of the project, including users of the audited contracts, owners or project investors.

## Some Other Thing

A reader of this document may want to know, such as non-trivial understandings required to do this audit or general comments regarding the project. An item regarding centralization and or upgradeability should usually go here.

# Changelog

* 2021-12-29 – Initial report based on commit xxxxx.
* 2022-01-06 – Reaudit report based on the fixes in commit xxxxx.

**Disclaimer: This audit report is not a security warranty, investment advice, or an approval of the NAME project since EatTheBlocks has not reviewed its platform. Moreover, it does not provide a smart contract code faultlessness guarantee.**