
CYBERCHAIN
FINANCE
AUDIT
CrogeZilla

CYBERCHAIN received a audit request

From CrogeZilla on April 14TH 2022

Attached is the information obtained
From the completed Audit.

Name: CrogeZilla

Contract address:
0x739c76e6d971acac8ff232c47bdf592446ee2072

Audit results:
Unknown veriables are not included

Audit: Passed

Ownership renounced: Not renounced

Kyc verified: Not verified

Audit number: Khn437bs
Audit team: CyberChain

Table of contents:

Audit Goal

To verify the smart contract system is secure.
And working according to specifications.

Security

Identifying security issues within
The contract and contract system.

Architecture

Evaluation of the system architecture.
Through lens of best general software practice's.

Primary areas of focus include
But are not limited to:

-readability
-accuracy
-high complexity sections
-quality of test coverage

Issue category's

-high level issue
-medium level issue
-low level issue

This audit report focuses on the security surrounding Pixle apes.
We are checking the reliability
And safeness of their smart contract. With a Thorough manual and auto audit process.

Audit methodology

The cyber chain team has performed thorough testing of the smart contract starting with assessing the code. We have reviewed the smart contract architecture to look for any manual flaws on the contract write.
Our team then conducted a line by line audit of the code.
We assessed for issue like race conditions,
Transactions ordering dependence,
time stamp dependence.

-testing to ensure proper logic
Has been followed throughout the code.

-testing complexity of the code
Manually line by line.
-analyze security of on chain data.

-asses for bugs and vulnerabilities.

Number of issues and severity type.
High level issue(0)/medium level issue(0)/ Result:
Low level issue(0)/

Project:

CrogeZilla

№	Assessment	Checking status
1	Compiler warnings.	Passed
2	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Zeppelin module.	Passed
21	Fallback function security.	Passed

Manual audit

Assessment by our Developers was made line by line.
Remix ide's was used to assist in testing process

High level issues

Zero issues found

Medium level issues

Zero issues found

Low level issues

Zero issues found

Automated audit

Remix compiler warning

Warning thrown by solidity compiler.
If it encounter’s any errors will not be able to deploy.
No issues found.

Disclaimer

This is a limited report of our findings,
In accordance with good industry standard.
This is in no way financial advice.
The information detailed is this report
Indicate our findings upon completion.
The automatic and manual findings
Found in this report are our personal opinion.
This information should not be used,
To determine investment opportunity's.
All information is in respect to the
Smart contract vulnerability
Reading this report is agreeing to the cyber chain
Term of service.
We hold zero liability for any loss of funds
Due to investing anywhere, at anytime.
No entity title member or employee
hold no duty of care.

Summary

Smart contract hold no high severity issues.
Please check disclaimer above and take note
The audit makes no statment of warranty on business model.

Thank you for reading
CYBERCHAIN finance