Paynch

Paynch received the application for a smart contract security audit of Snoopy AI Agent on May 15, 2025. The following are the details and results of this smart contract security audit:

Token Name: SNOOPY AI

Contract address: 0xf58F0090eb8964849872f1629EF83d70742a45ea

Link Address:
https://bscscan.com/token/0xf58F0090eb8964849872f1629EF83d70742a45ea

The audit items and results:
(Other unknown security vulnerabilities are not included in the audit responsibility scope)

Audit Result: Passed

Owner: Not renounced
(The contract contains ownership functionality and ownership is not renounced which allows the creator or current owner to modify contract behavior)

KYC Verification: Verified

Paynch

TABLE OF CONTENT

Paynch

INTRODUCTION

This Audit Report mainly focuses on the overall security of SNOOPY Airdrop Smart Contract. With this report, we have tried to ensure the reliability and correctness of their smart contract by complete and rigorous assessment of their system's architecture and the smart contract codebase.

AUDITING APPROACH AND METHODOLOGIES APPLIED

The Paynch team has performed rigorous testing of the project starting with analyzing the code design patterns in which we reviewed the smart contract architecture to ensure it is structured and safe use of third-party smart contracts and libraries.

Our team then performed a formal line by line inspection of the Smart Contract to find any potential issue like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks.

In the Unit testing Phase, we coded/conducted custom unit tests written for each function in the contract to verify that each function works as expected.

In Automated Testing, we tested the Smart Contract with our in-house developed tools to identify vulnerabilities and security flaws.

The code was tested in collaboration of our multiple team members and this included

- *Testing the functionality of the Smart Contract to determine proper logic has been followed throughout the whole process.*
- *Analyzing the complexity of the code in depth and detailed, manual review of the code, line-by-line.*
- *Deploying the code on testnet using multiple clients to run live tests.*
- *Analyzing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.*
- *Checking whether all the libraries used in the code are on the latest version.*
- *Analyzing the security of the on-chain data.*

AUDIT DETAILS

Project Name: Snoopy AI
Website: https://snoopybnb.wtf/
Platform: Binance Smart Chain
Type of Token: BEP20

Languages: Solidity (Smart contract)
Platforms and Tools: Remix IDE, Truffle, Truffle Team, Ganache, Solhint, VScode, Mythril

Paynch

AUDIT GOALS

The purpose of this audit is to analyze the smart contract responsible for the airdrop and user registration processes. The main objective is to identify any vulnerabilities or malicious logic that could harm users, such as functions that could drain their wallets or compromise their security.

SECURITY

Identifying security related issues within each contract and the system of contract.

SOUND ARCHITECTURE

Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.

CODE CORRECTNESS AND QUALITY

A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Sections of code with high complexity
- Quantity and quality of test coverage

ISSUE CATEGORIES

Every issue in this report was assigned a severity level from the following:

HIGH LEVEL SEVERITY ISSUES

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

MEDIUM LEVEL SEVERITY ISSUES

Issues on this level could potentially bring problems and should eventually be fixed.

LOW LEVEL SEVERITY ISSUES

Issues on this level are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.

Paynch

NUMBER OF ISSUES PER SEVERITY

Critical	High	Medium	Low	Note
0	0	0	0	0

ISSUES CHECKING STATUS

№	Issue description.	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

Paynch

MANUAL AUDIT:

For this section the code was tested/read line by line by our developers. We also used Remix IDE's JavaScript VM and Kovan networks to test the contract functionality.

CRITICAL SEVERITY ISSUES

No critical severity issues found.

HIGH SEVERITY ISSUES

No high severity issues found.

MEDIUM SEVERITY ISSUES

No medium severity issues found.

LOW SEVERITY ISSUES

No low severity issues found.

Paynch

AUTOMATED AUDIT

REMIX COMPILER WARNINGS

It throws warnings by Solidity’s compiler. If it encounters any errors the contract cannot be compiled and deployed. No issues found.

Paynch

DISCLAIMER

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Paynch

SUMMARY

Smart contracts do not contain any high severity issues.

Note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report.