



Shibance

Smart Contract Security Audit

Date 1/July/2021

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 disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and ApeAudits and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (ApeAudits) owe no duty of care towards you or any other person, nor does ApeAudits make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and ApeAudits hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, ApeAudits hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against ApeAudits, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

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.

Purpose

This document details ApeAudits' findings and recommended solutions. We performed a diff audit, which means we audited only the changes made to the original contracts (as the Shibance contracts are heavily based on PancakeSwap and ApeSwap contracts). This audit was performed on July 1, 2021. The contracts we audited are linked below. We also checked each contract's dependencies (such as libraries and external interfaces), which are listed in the BSCScan links. We audited only the links listed here.

Contract name(s)	Address
WoofVault	https://bscscan.com/address/0x09fe45a62502e7a0b226a99f18043f3ec32f78e8#code
Timelock	https://bscscan.com/address/0xb55ddb35cf6cb39662d6728757bb761c83d3d742#code
SupportBoi	https://bscscan.com/address/0x0703c295644ba1d333e14367e510773629264ee2#code
MasterBoi	https://bscscan.com/address/0x4fbee6d68b71ae4367f778129d4218668151eb99#code
DoggyPound	https://bscscan.com/address/0x516b3d832379cd9417bfa3cc54459460cb91fd33#code
WoofToken	https://bscscan.com/address/0x9e26c50b8a3b7652c3fd2b378252a8647a0c9268#code
ShibanceRouter + ShibanceLibrary	https://bscscan.com/address/0xa1fdb322ab5fe4df90099e6f514b9819aeaca8cf#code
ShibanceFactory + ShibancePair + ShibanceERC20	https://bscscan.com/address/0x092ee062baa0440b6df6bbb7db7e66d8902bdf7#code

Findings

NO.	Audit Items	Audit Subclass	Audit Subclass Result
1	Overflow Audit	N/A	Passed
2	Race Conditions Audit	N/A	Passed
3	Authority Control Audit	Permission Vulnerability Audit Excessive Auditing Authority	Passed Passed
4	Safe Design Audit	Zeppelin Module Safe Compiler Version Hard-coded Version Fallback Function Safeuse Show Coding Security Function Return Value Security Call Function Security	Passed Passed Passed Passed Passed Passed Passed
5	Denial of Service Audit	N/A	Passed
6	Gas Optimization Audit	N/A	Passed
7	Design Logic Audit	N/A	Passed
8	Malicious Event Log Audit	N/A	Passed
9	"False Deposit" Vulnerability Audit	N/A	Passed
10	Uninitialized Storage Pointers Audit	N/A	Passed
11	Arithmetic Accuracy Deviation Audit	N/A	Passed

High Severity Issues

- None.

Medium Severity Issues

- None.

Low Severity Issues

- **Issue:**
The Syrup exploit was unpatched and left in the code. However, the developers are aware of this and have stated that they will not give the DOGGYPOUND token any utility.

Recommendation:

The best course of action would be to patch the exploit or remove the vulnerable code entirely, but there will be no issue with keeping the code as long as the developers do not give DOGGYPOUND any value.

- Issue:

In ShibancePair.sol, at line 104 - multiplying the denominator by 10 causes the developers to receive 1/11 of the 0.3% liquidity fees (equating to ~0.02727% of transaction fees) instead of 1/3 (which would be 0.1% of transaction fees). For more information, see section 2.4 of the [Uniswap V2 whitepaper](#).

Recommendation:

This is not much of an issue, but it was unintended. It can either be patched or left the way it is. If left this way, liquidity providers will actually receive a larger percentage of rewards than they would normally.

Conclusion

No severe issues found. However, in the current state, the Syrup exploit has been left in. As long as the developers do not use DOGGYPOUND, this will not be an issue. Also, in the contract's current state, liquidity providers actually receive a small bonus to their liquidity rewards.

ApeAudits note:

Please check the disclaimer above and note, the audit is provided 'as-is' and makes no statements or warranties whatsoever. The report is provided only for the contract(s) mentioned in the report.

Appendix

Because of the volume of contracts, all supporting files can be found at <https://github.com/ApeAudits1/shibance-audit-extras>