SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

DECEMBER 2022

TTEB FINANCE

Kimberlite Safe

tteb.finance

Audit Details

Audited Project:

Kimberlite Safe

Deployer Wallet:

0xC95056c9c9f5CcaEbc2F343CB4fBc75BFf64Eb78

Client contacts:

Kimberlite Labs

Blockchain:

Dogechain

Project Links:

- WEBSITE
- TWITTER
- DISCORD

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 TTEB Finance and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TTEB Finance) owe no duty of care towards you or any other person, nor does TTEB Finance 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 TTEB Finance 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, TTEB Finance hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TTEB Finance, 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.

Background

TTEB Finance was commissioned by Kimberlite Labs to perform an audit of smart contracts implemented at https://explorer.dogechain.dog/address/0x1492AfF2D39fa5fFBF717DE80B15DCf3311B1BAb/

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified

Issues Checking Status

	Issue Description	Checking Status
1	Front running	Passed
2	Oracle calls	Passed
3	Compiler warnings	Passed
4	DoS with (Unexpected) Throw	Passed
5	Possible delays in data delivery	Passed
6	Timestamp dependence	Passed
7	Economy model of the contract	Passed
8	Private user data leaks	Passed
9	Malicious event log	Passed
10	DoS with block gas limit	Passed
11	Race conditions and reentrancy.	Passed
12	Integer Overflow and Underflow	Passed
13	Scoping and declarations.	Passed
14	Arithmetic accuracy	Passed

Issue Description(cont.)

15	Fallback function security	Passed
16	Cross-function race conditions.	Passed
17	Safe Open Zeppelin contracts implementation and usage.	Passed
18	Uninitialized storage pointers.	Passed
19	The impact of the exchange rate on the logic.	Passed
20	Design logic.	Passed
21	Methods execution permissions.	Passed
22	ERC20 API violation	Passed

Security Issues

✓ **High Severity Issues:**

No high severity issues found.

✓ **Medium Severity Issues:**

No medium severity issues found.

✓ **Low severity Issues:**

No low severity issues found.

Notes

KimberliteSafeUpgradeable is an upgradeable proxy managed by **`_admin`** and backed by the implementation at **`_logic`** using OpenZeppelin ERC1967Proxy transparent proxy implementation.

- **_admin** can upgrade the proxy contract or change the admin
- **authorized** addresses can can update fees

Recommendations

- Short Term: Timelock and Multi sign (⅔, ⅗) combination to avoid a single point of key management failure. Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations; AND assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key being compromised; AND a medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.
- Long Term: Timelock and DAO, the combination, mitigate by applying decentralization and transparency. Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations; AND Introduction of a DAO/governance/voting module to increase transparency and user involvement. AND a medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Conclusion

The **KimberliteSafe** smart contract contains no backdoors, and no scam scripts.

Security score: 91.

The code was tested with compatible compilers and manually reviewed for all commonly known and specific vulnerabilities. **KimberliteSafe** smart contract is safe for use on the Dogechain network.