ShieldAudit

SMART CONTRACT AUDIT REPORT

AUDIT DETAILS

CLIENT: zkhMaster Team

Contract Address:

0x3E32D92516a902C25171eD3Fbd81627958518cCf

Blockchain: zkSync

website: https://www.zkharvest.io/

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

ShieldAudits was commissioned by itself to perform an audit of smart contracts:

- https://explorer.zksync.io/address/0x3E32D92516a902C25171eD3Fbd81627958518cCf#contract

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.

ISSUE STATUS

ISSUE DESCRIPTION	CHECKING STATUS
Compiler errors.	**PASSED**
Race conditions and Re-entrancy. Cross-function race conditions	**PASSED**
Possible delays in data delivery.	**PASSED**
Oracle calls.	**PASSED**
Front running	**PASSED**
Timestamp dependence.	**PASSED**
Integer Overflow and Underflow.	**PASSED**
DoS with Revert	**PASSED**
DoS with block gas limit.	**LOW ISSUE**
Methods execution permissions.	**PASSED**
Economy model of the contract	**PASSED**
The impact of the exchange rate on the logic.	**PASSED**
Private user data leaks.	**PASSED**
Malicious Event log	**PASSED**
Scoping and Declarations	**PASSED**
Uninitialized storage pointers.	**PASSED**
Arithmetic accuracy.	**PASSED**
Design Logic.	**PASSED**
Cross-function race conditions	**PASSED**
Safe Open Zeppelin contracts implementation and usage.	**PASSED**
Fallback function security.	**PASSED**

SECURITY ISSUE

✓ **High Security Issues**
No high security issues found

✓ **Medium Security Issues**
No medium security issues found

✓ **Low Security Issues**
No low security issues found

Owner privileges (In the period when the owner is not renounced)

- ✓ **Owner can change setMasterEnabled value.**
- ✓ **Owner can transfer ownership.**
- ✓ **Owner and Dev address can change fee and NFT addresses.**
- ✓ **Owner and Dev address can set canSetNFT to false.**
- ✓ **Owner and Dev address can update emission rate.**
- ✓ **Owner and Dev address can change startTimestamp.**
- ✓ **Owner and Dev address can change BONUS_MULTIPLIER.**
- ✓ **Owner and Dev address can set NFT bonus data.**
- ✓ **Owner and Dev address can add/change pools.**

CONCLUSION

Smart contracts contain low security issues! The further transfers and operations with the funds raise are not related to this particular contract.

Security score: 77.

ShieldAudits 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 and does not include any other potential contracts deployed by Owner.