



AUDIT COMPANY



Elosys (ELO)

SMART CONTRACT SECURITY AUDIT

December 2023

CheckDot



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

CheckDot was commissioned by Elosys to perform an audit of smart contracts:

Mainnet Deployed Contract:

<https://etherscan.io/address/0x61b34A012646cD7357f58eE9c0160c6d0021fA41>

Github Repository: <https://github.com/Elosyslo/Wrapped-ELO-Token>

Github Repository Commit Hash: 6e6adcdb4d0b1a2c7f9a2457ae96c55920c00e26

Website: <https://elosys.io>

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. Compiler errors.	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 of the contract.	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 Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed
22. Fees detection	Passed



Contract Overview

PASSED

ELOSYS

(ELO)

DOES NOT SEEM LIKE A HONEYPOT

TOTAL SUPPLY

42,000,000 ELO

ADDRESS

OX61B34A012646CD7357F58EE9C0160C6D0021FA41

SIMULATION RESULTS

BUY TAX

0.0%

SELL TAX

0.0%

TRANSFER TAX

0.0%

BUY GAS

165,404

SELL GAS

118,995

SOURCE CODE

✓ OPEN SOURCE

BUY LIMIT

NONE

SELL LIMIT

NONE

Source code Verified on Etherscan.

0% Buy Internal Tax.

0% Sell Internal Tax.

No Buy Limit.

No Sell Limit.



Issues Categories

Total: [0 High, 0 Medium, 0 Low (2 fixed)]

✓ High Severity Issues

1. No issues.

✓ Medium Severity Issues

1. No issues

✓ Low Severity Issues

1. (Fixed) Using pragma 0.8.0, we advised using a more recent version solidity 0.8.20, which has been applied.
2. (Fixed) Initial offering details, but reported and corrected before deployment. (Look at the Token Distribution Section for more information.)



Token Distribution

The token distribution process in this ERC-20 token smart contract is a crucial component that allocates the initial supply of 42,000,000 ELO tokens to various wallets in accordance with predefined tokenomics. This distribution is a recommended practice applied by the project to fulfill various purposes, including liquidity provision, team incentives, development, strategic partnerships, reserves, and initiatives.

The distribution is executed within the contract's constructor function and is designed to ensure transparency, security, and adherence to the specified allocation percentages. Below, we provide an overview of the key wallets involved in the token distribution and the corresponding percentage allocations:

- 1. 75% (31,500,000) Elosys Launch Wallet:** This wallet is designated as the wallet for Elosys launch
0x5161E98658087B5DBacC9D14430DDa2a710541B0 receives 75% of the total supply, ensuring a significant portion of tokens for ->
55%:public sale - 23,100,000 \$ELO
20%: liquidity pool - 8,400,000 \$ELO
- 2. 15% (5,880,000) Team Treasury Wallet (_futureEndorsement):**
A wallet dedicated to prepare for events and when needed, such as for liquidity provision for CEX listings, receiving 10% of the total supply to incentivize long-term commitment and align interests with project success.
- 3. 10% (4,200,000) Development Fund Wallet**
(_coreTeamSupply): This wallet, allocated 10% of the total supply, is intended to support project development and growth.
- 4. 1% (420,000) Advisor Wallet (_advisorsSupply):** With 1% of the total supply, this wallet focuses on financing expertising provided by advisors who help the core team.



Extra functions

burn

In the context of this ERC-20 tokenized smart contract, the burn function serves as a powerful tool accessible to all. This function allows an ELO holder to burn ELO tokens, which will be destroyed when this feature is executed.

Security Considerations:

The burn function is rigorously secured. No fallback function is possible when burning tokens. In this way, the security and integrity of the ERC-20 smart token contract are effectively protected against unauthorized access and malicious actions. Nor can this function be used to modify the contract.



Conclusion

After a thorough examination of the smart contract code and its various components, it is reassuring to note that the contract has several essential security features. The code base is well structured, the import of the `@openzeppelin/contracts/token/ERC20` open-source library is very robust, and the code is well commented and very clear, making it easy to understand.

Transparent Token Distribution

The token distribution process is transparent and meticulously documented within the constructor function. The allocation percentages and the associated wallet addresses are clearly visible, providing transparency and accountability regarding how the initial supply of 42,000,000 ELO tokens is distributed among various purposes. Additionally, the emission of Transfer events during distribution further enhances transparency by creating an immutable ledger of token transfers.

Fee-Free Model

It is noteworthy that the smart contract operates on a fee-free model, as no fees or charges are associated with its functions. This simplicity aligns with the project's objective of ensuring a straightforward and cost-effective user experience.



In summary, the security level of this smart contract appears solid, with well-defined access controls, transparent token distribution and a clear, no-fee model. No vulnerabilities or issues were identified during our review. However, it is important to emphasize that code audits and security assessments should be an ongoing practice to adapt to evolving threats and maintain the long-term security of the contract. In addition, we had already discussed with this team to advise them on the best practices that were applied here, which led to a better finding.

Overall, the smart contract demonstrates a commendable commitment to security, transparency and usability, providing a solid foundation for the intended use in the deployment and management of ELO tokens.

CheckDot 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.