NOVOS

KYC & AUDIT.

Novos is an agency specializing in blockchain technology solutions, Audits, KYC / Doxx.

NOVOS

CERTIFICATE OF COMPLIANCE

Smart Contract Audit by NOVOS

ZukeSwap Router

Audit Passed

03/25/2023

NOVOS

Table of Contents

- Audit Summary
- Project Overview
- Main Contract Assessed
- Smart Contract Vulnerability Checks
- Contract Ownership
- Priviliged Functions
- Important Notes The Users
- Findings Summary
- Classification of Issues
- Findings Summary
- Classification of Issues
- Findings Table
- Public function that could be declared external
- Missing events arithmetic
- Statistics

NOVOS

Audit Summary

This report has been prepared for ZukeSwap Route on the Loop network. Novos provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

NOVOS

Project Overview

Parameter	Result
Address	0xeCaf4708d2027A071d24A32F4409E57f7cBACFA1
Name	ZukeRouter
Token Tracker	-
Decimals	-
Supply	-
Platform	Loop
Compiler	v0.6.6+commit.6c089d02
Optimization	True 200 runs
Other Settings:	default evmVersion
Language	Solidity
Codebase	https://explorer.mainnetloop.com/address/0xeCaf4708d2027A071d24A32F4409E57f7cBACFA1/contracts#address-tabs
Url	https://zukeswap.xyz/#/swap

Main Contract Assessed

Name	Contract	Live
ZukeRouter	0xeCaf4708d2027A071d24A32F4409E57f7cBACFA1	Yes

NOVOS

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
❖ Unencrypted Private Data On-Chain	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Code With No Effects	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Message call with hardcoded gas amount	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Hash Collisions With Multiple Variable Length Arguments	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unexpected Ether balance	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Presence of unused variables	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Right-To-Left-Override control character (U+202E)	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Typographical Error	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ DoS With Block Gas Limit	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Arbitrary Jump with Function Type Variable	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Insufficient Gas Griefing	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Incorrect Inheritance Order	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Write to Arbitrary Storage Location	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Requirement Violation	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Missing Protection against Signature Replay Attacks	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Weak Sources of Randomness from Chain Attributes	✓ Complete	✓ Complete	✓ **Low / No Risk**



NOVOS

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
❖ Authorization through tx.origin	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Delegatecall to Untrusted Callee	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Use of Deprecated Solidity Functions	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Assert Violation	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Reentrancy	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unprotected SELFDESTRUCT Instruction	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unprotected Ether Withdrawal	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unchecked Call Return Value	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Outdated Compiler Version	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Integer Overflow and Underflow	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Function Default Visibility	✓ Complete	✓ Complete	✓ **Low / No Risk**



NOVOS

Technical Findings Summary

Classification of Issues

Total

What you should pay attention to

Medium

Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.

High

Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency

Info

Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

Low

Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.

NOVOS

Findings

Here are some observations and suggestions based on analysis of the code

Description

Missing constructor visibility. The constructor for the ZukeRouter contract is missing the visibility modifier "public."

Recommendation

While this may not affect the functionality of the contract, it is a best practice to include the modifier to make the code more readable and explicit.

NOVOS

Findings

Here are some observations and suggestions based on analysis of the code

Description

Unused variables. The variables amountOut and path in the swapExactTokensForTokensSupportingFeeOnTransferTokens function are not used anywhere in the function, which may indicate that they are not necessary.

Recommendation

Consider removing them to simplify the code.

NOVOS

Findings

Here are some observations and suggestions based on analysis of the code

Description

No input validation. The swapExactETHForTokensSupportingFeeOnTransferTokens function does not validate the input parameters amountOutMin and path, which could potentially lead to errors or malicious behavior.

Recommendation

It is recommended to add input validation to ensure that the values provided by users are valid and within acceptable limits.

NOVOS

Findings

Here are some observations and suggestions based on analysis of the code

Description

Lack of inline comments. While the code is well-organized and readable, there are few inline comments explaining the purpose and functionality of certain sections of the code.

Recommendation

Consider adding more inline comments to make the code easier to understand for other developers.

NOVOS

Findings

Here are some observations and suggestions based on analysis of the code

Description

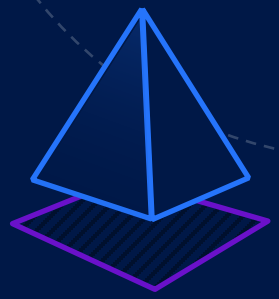
Use of external contracts. The contract uses two external contracts (IUniswapV2Router02 and IUniswapV2Factory) from the Uniswap V2 protocol.

Recommendation

It is important to ensure that these contracts are secure and audited, as any vulnerabilities in these contracts could also affect the security of the ZukeRouter contract.

NOVOS

Conclusion



Overall, the code for the ZukeRouter contract appears to be well-organized and functional. However, some minor improvements could be made to increase readability, simplify the code, and improve security. It is always recommended to have a professional audit to ensure the security and functionality of smart contracts in a production environment.

NOVOS

Disclaimer

Novos has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Novos is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Novos or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by Novos is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where- is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.