



**NOVOS**

## **KYC & AUDIT.**

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



# CERTIFICATE OF COMPLIANCE

Smart Contract Audit by NOVOS



ZukeSwap Factory

Audit Passed

03/31/2023

# Table of Contents

- ❖ **Audit Summary**
- ❖ **Project Overview**
- ❖ **Main Contract Assessed**
- ❖ **Smart Contract Vulnerability Checks**
- ❖ **Contract Ownership**
- ❖ **Privileged 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**



# Audit Summary

This report has been prepared for ZukeSwap Factory 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.



## Project Overview

Parameter	Result
Address	0xc738bE6fE1A54d7B0F6e4C3262a46a002aC2508e
Name	ZukeFactory
Token Tracker	-
Decimals	-
Supply	-
Platform	Loop
Compiler	v0.6.6+commit.6c089d02
Optimization	True 200 runs
Other Settings:	default evmVersion
Language	Solidity
Codebase	<a href="https://explorer.mainnetloop.com/address/0xc738bE6fE1A54d7B0F6e4C3262a46a002aC2508e/contracts">https://explorer.mainnetloop.com/address/0xc738bE6fE1A54d7B0F6e4C3262a46a002aC2508e/contracts</a>
Url	<a href="https://zukeswap.xyz/#/swap">https://zukeswap.xyz/#/swap</a>

## Main Contract Assessed

Name	Contract	Live
ZukeFactory	0xc738bE6fE1A54d7B0F6e4C3262a46a002aC2508e	Yes



# Smart Contract Vulnerability Checks

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





# Smart Contract Vulnerability Checks

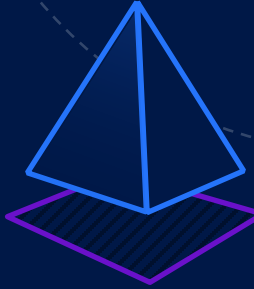
Vulnerability	Automatic Scan	Manual Scan	Result
❖ Authorization through tx.origin	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Delegatecall to Untrusted Callee	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Use of Deprecated Solidity Functions	✓ Complete	✓ Complete	✓ <b>Low / No Risk</b>
❖ Assert Violation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





NOVOS

## Observations:



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

- The code appears to be well-organized and documented.
- The Factory contract uses two external contracts (IUniswapV2Factory and IUniswapV2Pair) from the Uniswap V2 protocol, which need to be verified for security and audited.
- The functions in the contract appear to be working correctly and following the intended purpose.



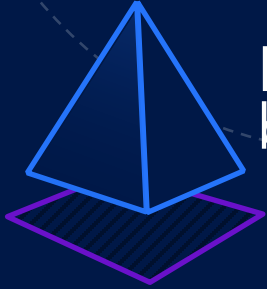




NOVOS

## Recommendations:

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

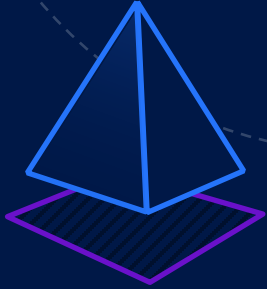


- Consider adding more inline comments to the code to make it easier to understand for other developers.
- Consider adding input validation for user-provided parameters to ensure that they are within acceptable limits.
- Consider adding checks to ensure that the tokens created through the Factory contract are unique and not already existing.
- Consider adding more tests to cover more edge cases and potential malicious attacks.



NOVOS

## Conclusion



In conclusion, the ZukeSwap Factory contract appears to be well-written and following its intended purpose. However, some minor improvements could be made to increase readability, simplify the code, and improve security. As always, it is recommended to have a professional audit to ensure the security and functionality of smart contracts in a production environment.



## 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 advocacy 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.