HACKEN

SMART CONTRACT CODE COMPARISON REPORT

Customer: HorizonDEX
Date: 11 July, 2023

Document

Name	Smart Contract Code Comparison Report for HorizonDEX
Type	ERC20 token; Pools
Platform	EVM
Language	Solidity
Methodology	Link
Website	-
Changelog	11.07.2023 - Initial Review

Table of contents

Introduction

Hacken OÜ (Consultant) was contracted by HorizonDEX (Customer) to conduct a Smart Contract Code Comparison. This report presents information about the conformity of a customer code with an original fork.

Scope

The scope of the project includes review and security analysis of the following smart contracts from the provided repository:

Initial review scope

Original Code	https://github.com/Horizon-Dex/contracts
Original Code Commit	888c8d2d6cb37e7b2e79eb2f5ce51551098d439a
Forked Code	https://github.com/KyberNetwork/ks-elastic-sc
Forked Code Commit	528ba22fb8d237790b187182bdc172be871ba225
Contracts	File: contracts/Factory.sol SHA3: 8c88970b517102ce6ae0086b5c0a665b8491325d2d0f6dd0160c616c468dd8c0 File: contracts/PoolStorage.sol SHA3: 1d58b9684bedbca511dec4e5e6185bd2a87aa0207eae2b69c2549d5543e8b7f8 File: contracts/Pool.sol SHA3: 50c0b03a0674223e77787fd93c8332cf2e437652322c3fc741feb61da2e78f30 File: contracts/PoolTicksState.sol SHA3: a7b6e71f443eb2285efd23a37653c2baa1784ed5ac740b412f3166ca5573b990

www.hacken.io

Executive Summary

The customer code is intended to be a fork of KyberSwap. All the differences, if any, are mentioned in the Difference section of the report, and their secureness and correctness cannot be guaranteed by this review.

Summary

The code is not an exact copy of the HorizonDex protocol.
During the review, auditors found 2 differences between the source of the fork and the fork itself.

Difference

D01. Added SwapFeeEnabled options

In the forked repo 3 additional fee swap options were added.

Path: ./contracts/Factory.sol : constructor()

Found in: 528ba22

D02. ERC20 name and symbol were changed

In the inheritance list, ERC20 arguments were changed.

Forked repo - ERC20('KyberSwap v2 Reinvestment Token', 'KS2-RT')

Main repo - ERC20("HorizonDEX Reinvestment Token", "HRZN-RT")

Path: ./contracts/Pool.sol : contract inheritance

Found in: 528ba22

Disclaimers

Hacken Disclaimer

The report contains no statements or warranties on the identification of all vulnerabilities and security of the code. The report covers the code submitted and reviewed, so it may not be relevant after any modifications. Do not consider this report as a final and sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements.

While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

English is the original language of the report. The Consultant is not responsible for the correctness of the translated versions.

Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the Consultant cannot guarantee the explicit security of the audited smart contracts.