PALADIN
BLOCKCHAIN SECURITY

Smart Contract Security Assessment

Final Report

For DragonSwap (v3)

01 August 2024

paladinsec.co

info@paladinsec.co

Table of Contents

Table of Contents 2

Disclaimer 3

1 Overview 4

1.1 Summary 5

2 Findings 6

2.1 General 6

Disclaimer

Paladin Blockchain Security ("Paladin") 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. Further, this audit report shall not be disclosed nor transmitted to any persons or parties on any objective, goal or justification without due written assent, acquiescence or approval by Paladin.

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 Paladin is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Paladin 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.

Cryptocurrencies and any technologies by extension directly or indirectly related to cryptocurrencies are highly volatile and speculative by nature. All reasonable due diligence and safeguards may yet be insufficient, and users should exercise considerable caution when participating in any shape or form in this nascent industry.

The audit report has made all reasonable attempts to provide clear and articulate recommendations to the Project team with respect to the rectification, amendment and/or revision of any highlighted issues, vulnerabilities or exploits within the contracts provided. It is the sole responsibility of the Project team to sufficiently test and perform checks, ensuring that the contracts are functioning as intended, specifically that the functions therein contained within said contracts have the desired intended effects, functionalities and outcomes of the Project team.

Paladin retains the right to re-use any and all knowledge and expertise gained during the audit process, including, but not limited to, vulnerabilities, bugs, or new attack vectors. Paladin is therefore allowed and expected to use this knowledge in subsequent audits and to inform any third party, who may or may not be our past or current clients, whose projects have similar vulnerabilities. Paladin is furthermore allowed to claim bug bounties from third-parties while doing so.

1 Overview

This report has been prepared for DragonSwap's DEX contracts on the SEI network. Paladin provides a user-centred examination of the smart contracts to look for vulnerabilities, logic errors or other issues from both an internal and external perspective.

This audit is a diff-audit, meaning we reviewed changes between DragonSwap's contracts and Uniswap's V3 contracts. More information is provided Below.

1.1 Summary

Project Name	DragonSwap
URL	https://dragonswap.app
Platform	SEI
Language	Solidity
DragonSwap Commits	https://github.com/dragonswap-app/v2-staker/tree/ca59d4713449402a7862b90f9899e4fbaa9bb46b https://github.com/dragonswap-app/deploy-v2/commit/81b911c045767499cbe5675e12beef83eb2193bc https://github.com/dragonswap-app/swap-router-contracts/commit/e6574f4d3da18768c5a533b465c11b01697d6ce3 https://github.com/dragonswap-app/v2-periphery/commit/da9d3a5491607b3e88a5133b7fd3c5c1f1f317eb https://github.com/dragonswap-app/v2-core/commit/77f934dd7182abf934787645d8b44057f61acf23
Uniswap V3 Commits	https://github.com/Uniswap/v3-staker/commit/6d06fe4034e4eec53e1e587fc4770286466f4b35 https://github.com/Uniswap/deploy-v3/commit/b7aac0f1c5353b36802dc0cf95c426d2ef0c3252 https://github.com/Uniswap/swap-router-contracts/tree/70bc2e40dfca294c1cea9bf67a4036732ee54303 https://github.com/Uniswap/v3-periphery/commit/0682387198a24c7cd63566a2c58398533860a5d1 https://github.com/Uniswap/v3-core/commit/d8b1c635c275d2a9450bd6a78f3fa2484fef73eb

2 Findings

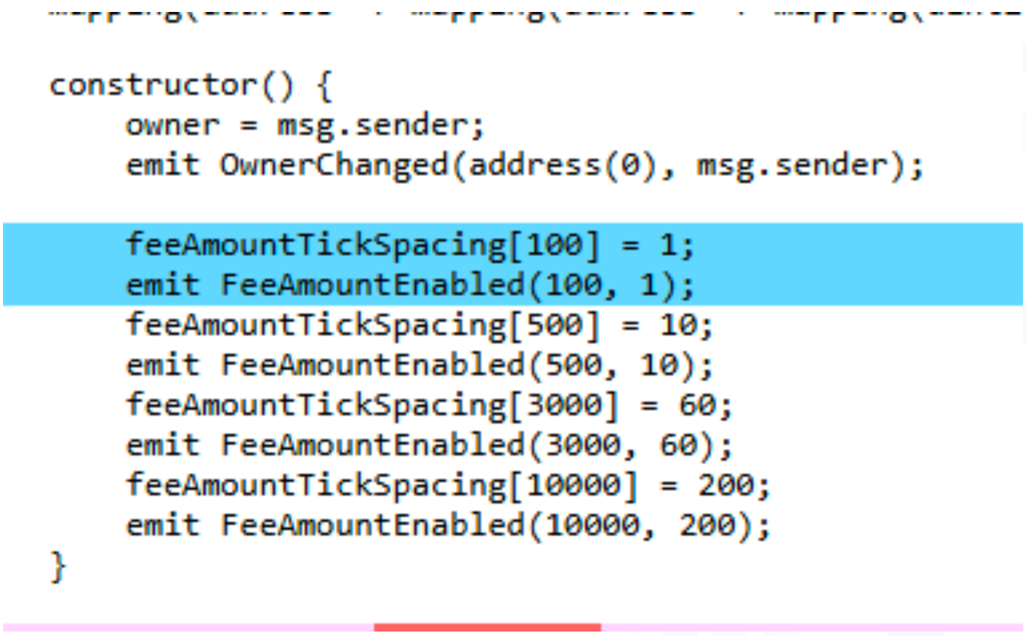
2.1 General

The repositories listed below have undergone a diff-audit by our team. The first column lists the Uniswap Repositories, and the second column lists the DragonSwap renamed versions.

Uniswap V3	DragonSwap
v3-core	v2-core
v3-periphery	v2-periphery
v3-staker	v2-staker
swap-router-contracts	swap-router-contracts
deploy-v3	deploy-v2

In all repositories, no issues have been found — most of the modifications are simply the renaming of uniswap to dragonswap.

We would like to note one change in DragonswapV2Factory where the 100 fee was added directly in the constructor and not in the deploy scripts.



```
constructor() {
    owner = msg.sender;
    emit OwnerChanged(address(0), msg.sender);

    feeAmountTickSpacing[100] = 1;
    emit FeeAmountEnabled(100, 1);
    feeAmountTickSpacing[500] = 10;
    emit FeeAmountEnabled(500, 10);
    feeAmountTickSpacing[3000] = 60;
    emit FeeAmountEnabled(3000, 60);
    feeAmountTickSpacing[10000] = 200;
    emit FeeAmountEnabled(10000, 200);
}
```

For every file below, we have provided the diff report between Uniswap and Dragonswap. The files can be found here: https://drive.google.com/drive/folders/1Li0NOGRFZ1mo_OcUV54yCBg2UBfOwT2-

v2-core

```
├── DragonswapV2Factory.sol
├── DragonswapV2Pool.sol
├── DragonswapV2PoolDeployer.sol
├── NoDelegateCall.sol
├── interfaces
│   ├── IDragonswapV2Factory.sol
│   ├── IDragonswapV2Pool.sol
│   ├── IDragonswapV2PoolDeployer.sol
│   ├── IERC20Minimal.sol
│   ├── callback
│   │   ├── IDragonswapV2FlashCallback.sol
│   │   ├── IDragonswapV2MintCallback.sol
│   │   └── IDragonswapV2SwapCallback.sol
│   └── pool
│       ├── IDragonswapV2PoolActions.sol
│       ├── IDragonswapV2PoolDerivedState.sol
│       ├── IDragonswapV2PoolEvents.sol
│       ├── IDragonswapV2PoolImmutables.sol
│       ├── IDragonswapV2PoolOwnerActions.sol
│       └── IDragonswapV2PoolState.sol
├── libraries
│   ├── BitMath.sol
│   ├── FixedPoint128.sol
│   ├── FixedPoint96.sol
│   ├── FullMath.sol
│   ├── LICENSE
│   ├── LICENSE_MIT
│   ├── LiquidityMath.sol
│   ├── LowGasSafeMath.sol
│   ├── Oracle.sol
│   ├── Position.sol
│   ├── SafeCast.sol
│   ├── SqrtPriceMath.sol
│   ├── SwapMath.sol
│   ├── Tick.sol
│   ├── TickBitmap.sol
│   ├── TickMath.sol
│   ├── TransferHelper.sol
│   └── UnsafeMath.sol
│
```

v2-periphery

```
├── NonfungiblePositionManager.sol
├── NonfungibleTokenPositionDescriptor.sol
├── SwapRouter.sol
├── V2Migrator.sol
├── base
│   ├── BlockTimestamp.sol
│   ├── ERC721Permit.sol
│   ├── LiquidityManagement.sol
│   ├── Multicall.sol
│   ├── PeripheryImmutableState.sol
│   ├── PeripheryPayments.sol
│   ├── PeripheryPaymentsWithFee.sol
│   ├── PeripheryValidation.sol
│   ├── PoolInitializer.sol
│   └── SelfPermit.sol
├── examples
│   └── PairFlash.sol
├── interfaces
│   ├── IERC20Metadata.sol
│   ├── IERC721Permit.sol
│   ├── IMulticall.sol
│   ├── INonfungiblePositionManager.sol
│   ├── INonfungibleTokenPositionDescriptor.sol
│   ├── IPeripheryImmutableState.sol
│   ├── IPeripheryPayments.sol
│   ├── IPeripheryPaymentsWithFee.sol
│   ├── IPoolInitializer.sol
│   ├── IQuoter.sol
│   ├── IQuoterV2.sol
│   ├── ISelfPermit.sol
│   ├── ISwapRouter.sol
│   ├── ITickLens.sol
│   ├── IV2Migrator.sol
│   └── external
│       ├── IERC1271.sol
│       ├── IERC20PermitAllowed.sol
│       └── IWSEI.sol
├── lens
│   ├── DragonswapInterfaceMulticall.sol
│   ├── Quoter.sol
│   ├── QuoterV2.sol
│   ├── README.md
│   └── TickLens.sol
├── libraries
│   ├── BytesLib.sol
│   ├── CallbackValidation.sol
│   ├── ChainId.sol
│   ├── HexStrings.sol
│   ├── LiquidityAmounts.sol
│   ├── NFTDescriptor.sol
│    ├── NFTSVG.sol
│    ├── OracleLibrary.sol
│    ├── Path.sol
│    ├── PoolAddress.sol
│    ├── PoolTicksCounter.sol
│    ├── PositionKey.sol
│    ├── PositionValue.sol
│    ├── SafeERC20Namer.sol
│    ├── SqrtPriceMathPartial.sol
│    └── TransferHelper.sol
```

v2-staker

```
├── DragonswapV2Staker.sol
├── interfaces
│    └── IDragonswapV2Staker.sol
├── libraries
│    ├── IncentiveId.sol
│    ├── NFTPositionInfo.sol
│    ├── RewardMath.sol
│    └── TransferHelperExtended.sol
```

swap-router-contracts

```
├── SwapRouter02.sol
├── V1SwapRouter.sol
├── V2SwapRouter.sol
├── base
│   ├── ApproveAndCall.sol
│   ├── ImmutableState.sol
│   ├── MulticallExtended.sol
│   ├── OracleSlippage.sol
│   ├── PeripheryPaymentsExtended.sol
│   ├── PeripheryPaymentsWithFeeExtended.sol
│   └── PeripheryValidationExtended.sol
├── interfaces
│   ├── IApproveAndCall.sol
│   ├── IImmutableState.sol
│   ├── IMixedRouteQuoterV1.sol
│   ├── IMulticallExtended.sol
│   ├── IOracleSlippage.sol
│   ├── IPeripheryPaymentsExtended.sol
│   ├── IPeripheryPaymentsWithFeeExtended.sol
│   ├── IQuoter.sol
│   ├── IQuoterV2.sol
│   ├── ISwapRouter02.sol
│   ├── ITokenValidator.sol
│   ├── IV1SwapRouter.sol
│   └── IV2SwapRouter.sol
├── lens
│   ├── MixedRouteQuoterV1.sol
│   ├── Quoter.sol
│   ├── QuoterV2.sol
│   ├── README.md
│   └── TokenValidator.sol
├── libraries
│   ├── Constants.sol
│   ├── DragonswapLibrary.sol
│   └── PoolTicksCounter.sol
│
```

deploy-v2

```
├── deploy.ts
├── migrate.ts
├── migrations.ts
├── steps
│   ├── deploy-multicall2.ts
│   ├── deploy-nft-descriptor-library.ts
│   ├── deploy-nft-position-descriptor.ts
│   ├── deploy-nonfungible-position-manager.ts
│   ├── deploy-proxy-admin.ts
│   ├── deploy-quoter-v2.ts
│   ├── deploy-tick-lens.ts
│   ├── deploy-transparent-proxy-descriptor.ts
│   ├── deploy-v2-core-factory.ts
│   ├── deploy-v2-migrator.ts
│   ├── deploy-v2-staker.ts
│   ├── deploy-v2-swap-router-02.ts
│   ├── meta
│   │   ├── createDeployContractStep.ts
│   │   └── createDeployLibraryStep.ts
│   ├── transfer-proxy-admin.ts
│   └── transfer-v2-core-factory-owner.ts
└── util
    ├── asciiStringToBytes32.ts
    └── linkLibraries.ts
```

PALADIN

BLOCKCHAIN SECURITY