Six Network

Definix Periphery

Security Assessment

March 29th, 2021

Audited By:
Alex Papageorgiou @ CertiK
alex.papageorgiou@certik.org
Reviewed By:
Camden Smallwood @ CertiK
camden.smallwood@certik.org

Disclaimer

CertiK reports are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security review.

CertiK Reports do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

CertiK Reports should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

CertiK Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

What is a CertiK report?

- A document describing in detail an in depth analysis of a particular piece(s) of source code provided to CertiK by a Client.
- An organized collection of testing results, analysis and inferences made about the structure, implementation and overall best practices of a particular piece of source code.
- Representation that a Client of CertiK has completed a round of auditing with the intention to increase the quality of the company/product's IT infrastructure and or source code.

Overview

Project Summary

Project Name	Six Network - Definix Periphery
Description	The periphery contracts of the DEX Definix implementation.
Platform	Ethereum; Solidity, Yul
Codebase	GitHub Repository
Commits	1. 9cbc5e3050a4a8e0502d8136c59a30ec369d291f

Audit Summary

Delivery Date	March 29th, 2021
Method of Audit	Static Analysis, Manual Review
Consultants Engaged	1
Timeline	March 26th, 2021 - March 29th, 2021

Vulnerability Summary

Total Issues	1
● **Total Critical**	0
● **Total Major**	0
● **Total Medium**	0
● **Total Minor**	0
● **Total Informational**	1

Executive Summary

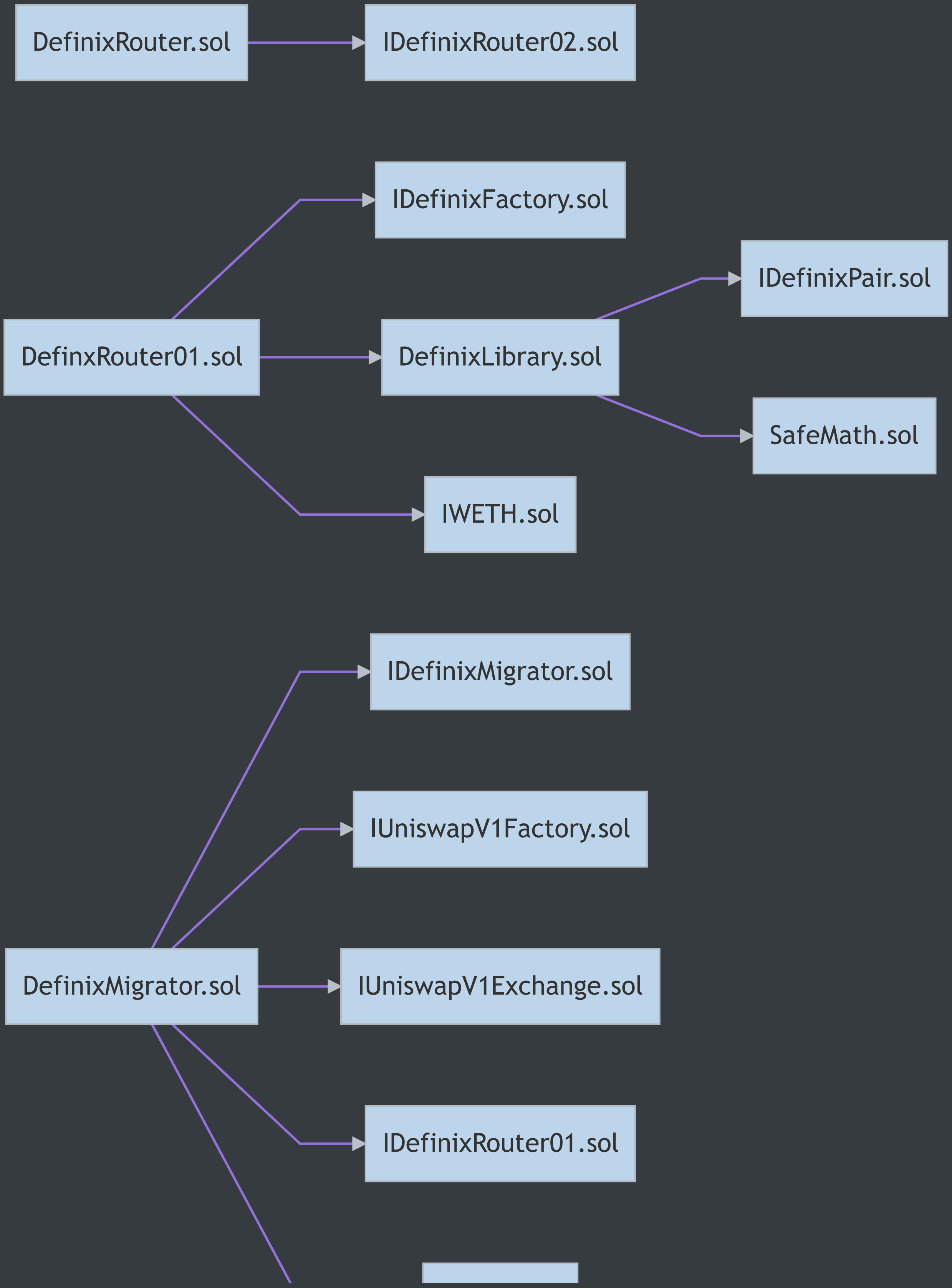
We were tasked with auditing the Definix repository of periphery contracts that are meant to interface with the DEX implementation and are based on PancakeSwap which in turn is based on Uniswap.

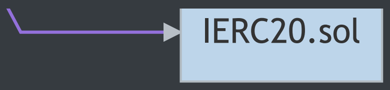
No changes were observed in the codebase that alter the functionality of the contracts apart from an adjustment to the init code of the `CREATE2` address calculation. We have noted that this init code hash should be validated prior to launch to ensure that the address calculations perform as expected.

Files In Scope

ID	Contract	Location
DMR	DefinixMigrator.sol	contracts/DefinixMigrator.sol
DRR	DefinixRouter.sol	contracts/DefinixRouter.sol
DR1	DefinxRouter01.sol	contracts/DefinxRouter01.sol
IDF	IDefinixFactory.sol	contracts/interfaces/IDefinixFactory.sol
IDM	IDefinixMigrator.sol	contracts/interfaces/IDefinixMigrator.sol
IDP	IDefinixPair.sol	contracts/interfaces/IDefinixPair.sol
IDR	IDefinixRouter01.sol	contracts/interfaces/IDefinixRouter01.sol
CON	IDefinixRouter02.sol	contracts/interfaces/IDefinixRouter02.sol
IER	IERC20.sol	contracts/interfaces/IERC20.sol
IWE	IWETH.sol	contracts/interfaces/IWETH.sol
DLY	DefinixLibrary.sol	contracts/libraries/DefinixLibrary.sol
SMH	SafeMath.sol	contracts/libraries/SafeMath.sol
IUE	IUniswapV1Exchange.sol	contracts/interfaces/V1/IUniswapV1Exchange.sol
IUV	IUniswapV1Factory.sol	contracts/interfaces/V1/IUniswapV1Factory.sol

File Dependency Graph





IERC20.sol

Manual Review Findings

ID	Title	Type	Severity	Resolved
DLY-01	Hardcoded Init Hash	Language Specific	● Informational	❕

DLY-01: Hardcoded Init Hash

Type	Severity	Location
Language Specific	● Informational	DefinixLibrary.sol L24

Description:

The init hash used in the calculation of the `CREATE2` address of a pair is hardcoded in the codebase.

Recommendation:

We advise this to be validated prior to launch as slight adjustments in the codebase can alter the init code hash and thus cause this calculation to fail.

Alleviation:

The Six Network - Definix Periphery development team has acknowledged this exhibit but decided to not apply its remediation in the current version of the codebase due to time constraints.

Appendix

Finding Categories

Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of `private` or `delete`.