verichains

SECURITY AUDIT OF

BASEMAXFI SMART CONTRACT

Public Report

Nov 20, 2023

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
Solidity	A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform.
Solc	A compiler for Solidity.
ERC20	ERC20 (BEP20 in Binance Smart Chain or *x*RP20 in other chains) tokens are blockchain-based assets that have value and can be sent and received. The primary difference with the primary coin is that instead of running on their own blockchain, ERC20 tokens are issued on a network that supports smart contracts such as Ethereum or Binance Smart Chain.

EXECUTIVE SUMMARY

This Security Audit Report prepared by Verichains Lab on Nov 20, 2023. We would like to thank Basemaxfi for trusting Verichains Lab, delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the Basemaxfi Smart Contract. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team had identified no vulnerable issue in the project source code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Basemaxfi Smart Contract

BaseMax isn't just a platform; it's a decentralized perpetuals trading powerhouse, putting the DeFi revolution at your fingertips. Dive into a sea of synthetic assets.

1.2. Audit scope

In this particular project, a timebox approach was used to define the consulting effort. This means that **Verichains Lab** allotted a prearranged amount of time to identify and document vulnerabilities. Because of this, there is no guarantee that the project has discovered all possible vulnerabilities and risks.

Furthermore, the security check is only an immediate evaluation of the situation at the time the check was performed. An evaluation of future security levels or possible future risks or vulnerabilities may not be derived from it.

This audit focused on identifying security flaws in code and the design of the Basemaxfi Smart Contract. The scope of the audit is limited to the source code files provided to Verichains. It was conducted on commit `808efcd0be90210e334ecdd89b8afe2f374091d2` from git repository *https://github.com/basemaxfi/basemax-contracts/tree/main*.

1.3. Audit methodology

Our security audit process includes four steps:

- Mechanism Design is reviewed to look for any potential problems.
- Source codes are scanned/tested for commonly known and more specific vulnerabilities using public and our in-house security analysis tool.
- Manual audit of the codes for security issues. The source code is manually analyzed to look for any potential problems.
- Set up a testing environment to debug/analyze found issues and verifies our attack PoCs.

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the functioning; creates a critical risk to the application; required to be fixed immediately.

SEVERITY LEVEL	DESCRIPTION
HIGH	A vulnerability that could affect the desired outcome of executing the application with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the application with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 1. Severity levels

1.4. Disclaimer

Basemaxfi acknowledges that the security services provided by Verichains, are conducted to the best of their professional abilities but cannot guarantee 100% coverage of all security vulnerabilities. Basemaxfi understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, Basemaxfi agrees that Verichains shall not be held responsible or liable, and shall not be charged for any hacking incidents that occur due to security vulnerabilities not identified during the audit process.

1.5. Acceptance Minute

This final report served by Verichains to the Basemaxfi will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the Basemaxfi, the final report will be considered fully accepted by the Basemaxfi without the signature.

2. AUDIT RESULT

2.1. Overview

The Basemaxfi Smart Contract is built based on the Vela Exchange which is an open source project. This project is a fork from Vela Exchange project at Arbitrum:

Below is the list of smart contracts for the Vela Exchange project:

Name	Contract Address
VUSD	0xAA0B397B0896A864714dE56AA33E3df471229268
VLP	0xC5b2D9FDa8A82E8DcECD5e9e6e99b78a9188eB05
Vela	0x088cd8f5ef3652623c22d48b1605dcfe860cd704
esVELA	0xeFD5A713C5bd85e9Ced46070b2532E4a47a18102
vault	0xC4ABADE3a15064F9E3596943c699032748b13352
liquidateVault	0x361A5F8fA6860B5f5C021A5Dd370C1180010A561
orderVault	0x52AC3eda13EB7959f918Df02a72d0f6c9C703523
positionVault	0x8B97E18eE706d056A5659947a717A7971003f524
tokenFarm	0x60b8C145235A31f1949a831803768bF37d7Ab7AA
settingsManager	0x6F2c6010A438546242cAb29Bb755c1F0AfaCa5AA
priceManager	0xC8e027C40B25C4Cd0c059763D042e79466D7bBB6
complexRewardPerSec1	0x40c3bD6D4A07117fcE69B60Eb1d446984e0a1383
Reader	0x18b38d25F301a157e17358301CdD41Cc18515B4A
SwapAndAirdrop	0xeFB4FF63DA3dAd854Aa339c1Ea2D96BbA831364d
Operators	0x23fc7c88402Fe3314d4E76AC42F4c5A3e01aE684
tokenDistributeRewarder	0x8DFC8C7D8A8A8cEf0bA7d6738a063C0b5adFdDdd

Table 2. The Vela Exchange Smart Contracts

Below is the list of addresses of implementations for the proxy contracts of Vela Exchange:

Name	Contract Address
vault	0x2a11233ad9f5Bb6567f96CA1c5c446F983194D0b
liquidateVault	0xBE99A1FF09C1A9f64f9cF85C4821f4d1EfAB49A0
orderVault	0x5559F2cb163c53F0DAe64020f8b50fA672293a31
positionVault	0x45131539295eB1b39587cceF8df19227229D4B2e
tokenFarm	0xCF4b3E952720BbfFB8985edbA20C5743a04E13ca
settingsManager	0xd6bCB485e05c7dc318A26890a582f023B6743F51
priceManager	0x7C1b0E6b6D408911bdB773136D28e4aD05C7692B
complexRewardPerSec1	0xC13f6696F9DC945Dc74f79Ee88D4cB4A7ECfFe71
Reader	0xf41DFF475922BC611aF0Ec1107a142A0A4cc6d2A
SwapAndAirdrop	0xFda366965aEadA2F3Fd32645945194C53d2694D0

Table 3. The Vela Exchange Smart Contract Implementations

The differences between the Basemaxfi Smart Contract and the VelaExchange are summarized below:

- Add the `Multicall` contract, with the main function being the `aggregate()` function that can be called by anyone. This function will execute external calls based on the caller's requests.
- Add the `OrderExecutor` contract, where the order functions can be called by an operator with a minimum level of 1.
- Remove the 2 contracts, `SwapAndAirdrop` and `TokenRewardDistributor` contracts.

These changes do not make any serious impact on the security design of the Basemaxfi Smart Contract.

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of Basemaxfi Smart Contract.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Nov 20, 2023*	Public Report	Verichains Lab

Table 4. Report versions history