AUDITS

SECURITY ASSESSMENT

BASE PROTOCOL

AUGUST 25TH 2022

TABLE OF CONTENTS

1 LEGAL DISCLAIMER

2 MH AUDITS INTRO

3 PROJECT SUMMARY

4 AUDIT SCORES

5 AUDIT SCOPE

6 METHODOLOGY

7 KEY FINDINGS

8 VULNERABILITIES

9 SOURCE CODE

10 APPENDIX

LEGAL DISCLAIMER

MH Audits 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 MH Audits to perform a security review.

MH Audits does 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.

MH Audits 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.

The report is provided only for the contract(s) mentioned in the report and does not include any other potential additions and/or contracts deployed by Owner. The report does not provide a review for contract(s), applications and/or operations, that are out of this report scope.

MH Audits' 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.

MH Audits represents 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. MH Audits' position is that each company and individual are responsible for their own due diligence and continuous security.

The security audit is not meant to replace functional testing done before a software release. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent manual audits and a public bug bounty program to ensure the security of the smart contracts.

INTRODUCTION

MH Audits is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

Secure your project with MH Audits

We offer field-proven audits with in-depth reporting and a range of suggestions to improve and avoid contract vulnerabilities.

Industry-leading comprehensive and transparent smart contract auditing on all public and private blockchains.

Vunerability checking

A crucial manual inspection carried out to eliminate any code flaws and security loopholes. This is vital to avoid vulnerabilities and exposures incurring costly errors at a later stage.

Contract verification

A thorough and comprehensive review in order to verify the safety of a smart contract and ensure it is ready for launch and built to protect the end-user.

Risk assessment

Analyse the architecture of the blockchain system to evaluate, assess and eliminate probable security breaches. This includes a full assessment of risk and a list of expert suggestions.

In-depth reporting

A truly custom exhaustive report that is transparent and depicts details of any identified threats and vulnerabilities and classifies those by severity.

Fast turnaround

We know that your time is valuable and therefore provide you with the fastest turnaround times in the industry to ensure that both your project and community are at ease.

Best-of-class blockchain engineers

Our engineers combine both experience and knowledge stemming from a large pool of developers at our disposal. We work with some of the brightest minds that have audited countless smart contracts over the last 4 years.

PROJECT SUMMARY

PROJECT INTRODUCTION

Base Protocol are building the front page of Cube Network, utilizing the chain's unique characteristics to create an ultra-fast AMM dex, an innovative launchpad with SAFT derivatives, an order-book based dex, and more.

The core of any DeFi ecosystem is the AMM Dex. Having taken off in Summer 2020, Base recognize that this is the first place that any DeFi participant will go, whether it's to swap, pool, or farm. As such, the AMM is the first product that Base will ship, becoming the cornerstone application on Cube Network for investors, traders, and speculators. The high scalability of Cube Network, combined with the built-in ZK-Rollups, will allow for the fastest swaps on any EVM chain.

Project Name *Base Protocol*

Contract Name *BASE Token*

Contract Address -

Contract Chain *Not Yet Deployed on Mainnet*

Contract Type *Smart Contract*

Platform *EVM*

Language *Solidity*

Codebase *GitHub Repository*

INFO & SOCIALS

Network *CUBE Network (CRC20)*

Total Supply *300,000,000*

Website *https://baseprotocol.io/*

Twitter *https://twitter.com/baseprotocolIO*

Telegram Chat *https://t.me/baseprotocolio*

Telegram Ann -

Medium *https://medium.com/@BaseProtocolIO*

CubeScan -

AUDIT SCORES

Issues	1
Critical	0
Major	0
Medium	0
Minor	1
Informational	0
Discussion	0

All issues are described in further detail on the following pages.

AUDIT SCOPE

FILE	LOCATION
IUniswapV2Factory.sol	*Private GitHub Repository*
IUniswapV2Router01.sol	*Private GitHub Repository*

REVIEW METHODOLOGY

TECHNIQUES

This report has been prepared for Base Protocol to discover issues and vulnerabilities in the source code of the Base Protocol project as well as any contract dependencies that were not part of an officially recognized library.

Project Engagement - On 19th of August 202, Base Protocol team engaged MH Audits to audit the smart contracts that they created, as described in this report's audit scope. The engagement was technical in nature and focused on identifying the security flaws in the design and specifically implementation of the interfaces. They provided MH Audits access to their GitHub repository.

MH Audits is not liable for any other aspect of the code represented by them other than the implementation of the interface referenced in this report

We have concluded that the interfaces were defined correctly.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Thorough line-by-line manual review of the entire codebase by industry experts.

TIMESTAMP

Version	v1.0
Date	2022/08/25
Description	Layout project
	Automated / Manual review / Interfaces check
	Summary

KEY FINDINGS

TITLE	SEVERITY	STATUS
Floating Pragma	Minor	*Pending*

Description: *Locking the pragma helps ensure that the contracts do not accidentally get deployed using an older version of the Solidity compiler affected by vulnerabilities.*

The contracts found in the repository were allowing floating or unlocked pragma to be used, i.e., ^0.8.0 *This allows the contracts to be compiled with all the solidity compiler versions above* 0.8.0*. The following contracts were found to be affected:*

Location: *IUniswapV2Router01.sol - L03*
IUniswapV2Factory.sol - L03

Impacts: *If the smart contract gets compiled and deployed with an older or too recent version of the solidity compiler, there's a chance that it may get compromised due to the bugs present in the older versions or unidentified exploits in the new versions.*

Incompatibility issues may also arise if the contract code does not support features in other compiler versions, therefore, breaking the logic.

The likelihood of exploitation is really low therefore this is only informational.

Issue: *Floating Pragma*

Type: *Floating Pragma (SWC-103)*

Level: *Minor*

Recommendation: *Keep the compiler versions consistent in all the smart contract files. Do not allow floating pragmas anywhere. It is suggested to use* 0.8.7 *pragma version*

Reference: https://swcregistry.io/docs/SWC-103

Alleviation:

Private GitHub Repository

FINDING CATEGORIES

The assessment process will utilize a mixture of static analysis, dynamic analysis, in-depth manual review and/or other security techniques.

This report has been prepared for Base Protocol project using the above techniques to examine and discover vulnerabilities and safe coding practices in Base Protocol's smart contract including the libraries used by the contract that are not officially recognized.

A comprehensive static and dynamic analysis has been performed on the solidity code in order to find vulnerabilities ranging from minor gas optimizations to major vulnerabilities leading to the loss of funds.

Various common and uncommon attack vectors will be investigated to ensure that the smart contracts are secure from malicious actors. The testing methods find and flag issues related to gas optimizations that help in reducing the overall gas cost It scans and evaluates the codebase against industry best practices and standards to ensure compliance It makes sure that the officially recognized libraries used in the code are secure and up to date.

AUDIT SCORES

MH Audits AuditScores is not a live dynamic score. It is a fixed value determined at the time of the report issuance date.

MH Audits AuditScores are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports and scores 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 MH Audits to perform a security review.

AUDITS

WEBSITE
MHAUDITS.IO

TWITTER
@MHAUDITS