BaryonSwap

Smart Contract Audit Report
Prepared for Baryon Network

Date Issued:	Jan 13, 2022
Project ID:	AUDIT2021050
Version:	v1.0
Confidentiality Level:	Public

inspex
CYBERSECURITY PROFESSIONAL SERVICE

Report Information

Project ID	AUDIT2021050
Version	v1.0
Client	Baryon Network
Project	Factory & Router
Auditor(s)	Weerawat Pawanawiwat Patipon Suwanbol
Author	Patipon Suwanbol
Reviewer	Suvicha Buakhom
Confidentiality Level	Public

Version History

Version	Date	Description	Author(s)
1.0	Jan 13, 2022	Full report	Patipon Suwanbol

Contact Information

Company	Inspex
Phone	(+66) 90 888 7186
Telegram	t.me/inspexco
Email	audit@inspex.co

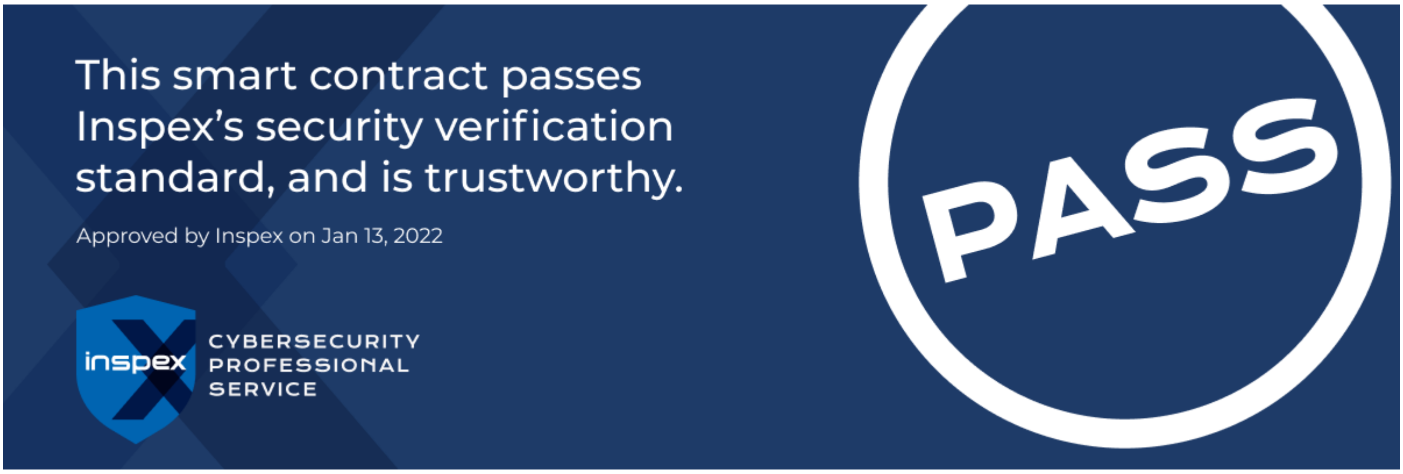
Table of Contents

1. Executive Summary

As requested by Baryon Network, Inspex team conducted an audit to verify the security posture of the BaryonSwap smart contracts on Jan 5, 2022. During the audit, Inspex team examined all smart contracts and the overall operation within the scope to understand the overview of BaryonSwap smart contracts. Static code analysis, dynamic analysis, and manual review were done in conjunction to identify smart contract vulnerabilities together with technical & business logic flaws that may be exposed to the potential risk of the platform and the ecosystem. Practical recommendations are provided according to each vulnerability found and should be followed to remediate the issue.

1.1. Audit Result

In the initial audit, Inspex found 1 very low-severity issue. With the project team's prompt response, the issue was resolved in the reassessment. Therefore, Inspex trusts that BaryonSwap smart contracts have high-level protections in place to be safe from most attacks.



This smart contract passes Inspex's security verification standard, and is trustworthy.

Approved by Inspex on Jan 13, 2022

inspex
CYBERSECURITY PROFESSIONAL SERVICE
PASS

1.2. Disclaimer

This security audit is not produced to supplant any other type of assessment and does not guarantee the discovery of all security vulnerabilities within the scope of the assessment. However, we warrant that this audit is conducted with goodwill, professional approach, and competence. Since an assessment from one single party cannot be confirmed to cover all possible issues within the smart contract(s), Inspex suggests conducting multiple independent assessments to minimize the risks. Lastly, nothing contained in this audit report should be considered as investment advice.

2. Project Overview

2.1. Project Introduction

BaryonSwap is an Automated Market Maker (AMM) protocol that is forked from Uniswap V2 and launched on the Binance Smart Chain (BSC).

With BaryonSwap contracts, users can perform ERC20 token swapping easily with the liquidity pool of the platform. Users can also provide liquidity to the pools and gain a part of the swapping fee and the platform's reward tokens.

Scope Information:

Project Name	BaryonSwap
Website	https://www.baryon.network/swap
Smart Contract Type	Ethereum Smart Contract
Chain	Binance Smart Chain
Programming Language	Solidity

Audit Information:

Audit Method	Whitebox
Audit Date	Jan 5, 2022
Reassessment Date	Jan 12, 2022

The audit method can be categorized into two types depending on the assessment targets provided:

1. **Whitebox**: The complete source code of the smart contracts are provided for the assessment.
2. **Blackbox**: Only the bytecodes of the smart contracts are provided for the assessment.

2.2. Scope

The following smart contracts were audited and reassessed by Inspex in detail:

Initial Audit: (Commit: 230983c16666233811847eac92220142682748f2)

Contract	Location (URL)
BaryonFactory	https://github.com/coin98/baryon-swap/blob/230983c166/contracts/BaryonFactory.sol
BaryonRouter	https://github.com/coin98/baryon-swap/blob/230983c166/contracts/BaryonRouter.sol

Reassessment: (Commit: c717b1e70dcc2010201a49524a6b940904f8d0cf)

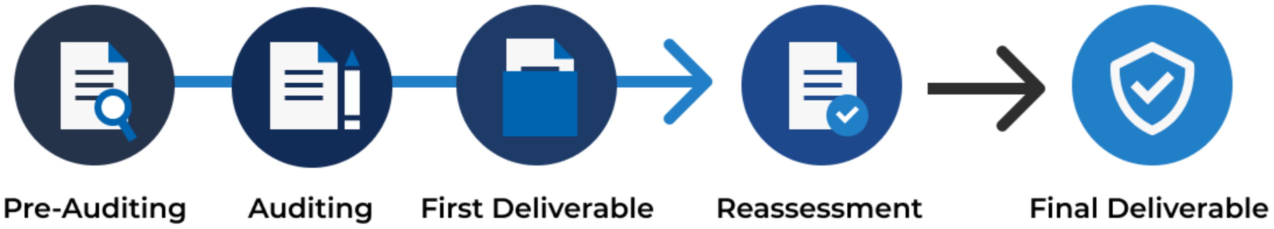
Contract	Location (URL)
BaryonFactory	https://github.com/coin98/baryon-swap/blob/c717b1e70d/contracts/BaryonFactory.sol
BaryonRouter	https://github.com/coin98/baryon-swap/blob/c717b1e70d/contracts/BaryonRouter.sol

The assessment scope covers only the in-scope smart contracts and the smart contracts that they inherit from.

3. Methodology

Inspex conducts the following procedure to enhance the security level of our clients' smart contracts:

1. **Pre-Auditing**: Getting to understand the overall operations of the related smart contracts, checking for readiness, and preparing for the auditing
2. **Auditing**: Inspecting the smart contracts using automated analysis tools and manual analysis by a team of professionals
3. **First Deliverable and Consulting**: Delivering a preliminary report on the findings with suggestions on how to remediate those issues and providing consultation
4. **Reassessment**: Verifying the status of the issues and whether there are any other complications in the fixes applied
5. **Final Deliverable**: Providing a full report with the detailed status of each issue



3.1. Test Categories

Inspex smart contract auditing methodology consists of both automated testing with scanning tools and manual testing by experienced testers. We have categorized the tests into 3 categories as follows:

1. **General Smart Contract Vulnerability (General)** - Smart contracts are analyzed automatically using static code analysis tools for general smart contract coding bugs, which are then verified manually to remove all false positives generated.
2. **Advanced Smart Contract Vulnerability (Advanced)** - The workflow, logic, and the actual behavior of the smart contracts are manually analyzed in-depth to determine any flaws that can cause technical or business damage to the smart contracts or the users of the smart contracts.
3. **Smart Contract Best Practice (Best Practice)** - The code of smart contracts is then analyzed from the development perspective, providing suggestions to improve the overall code quality using standardized best practices.

3.2. Audit Items

The following audit items were checked during the auditing activity.

General
Reentrancy Attack
Integer Overflows and Underflows
Unchecked Return Values for Low-Level Calls
Bad Randomness
Transaction Ordering Dependence
Time Manipulation
Short Address Attack
Outdated Compiler Version
Use of Known Vulnerable Component
Deprecated Solidity Features
Use of Deprecated Component
Loop with High Gas Consumption
Unauthorized Self-destruct
Redundant Fallback Function
Insufficient Logging for Privileged Functions
Invoking of Unreliable Smart Contract
Use of Upgradable Contract Design
Advanced
Business Logic Flaw
Ownership Takeover
Broken Access Control
Broken Authentication
Improper Kill-Switch Mechanism

Improper Front-end Integration
Insecure Smart Contract Initiation
Denial of Service
Improper Oracle Usage
Memory Corruption
Best Practice
Use of Variadic Byte Array
Implicit Compiler Version
Implicit Visibility Level
Implicit Type Inference
Function Declaration Inconsistency
Token API Violation
Best Practices Violation

3.3. Risk Rating

OWASP Risk Rating Methodology[1] is used to determine the severity of each issue with the following criteria:

- **Likelihood**: a measure of how likely this vulnerability is to be uncovered and exploited by an attacker.
- **Impact**: a measure of the damage caused by a successful attack

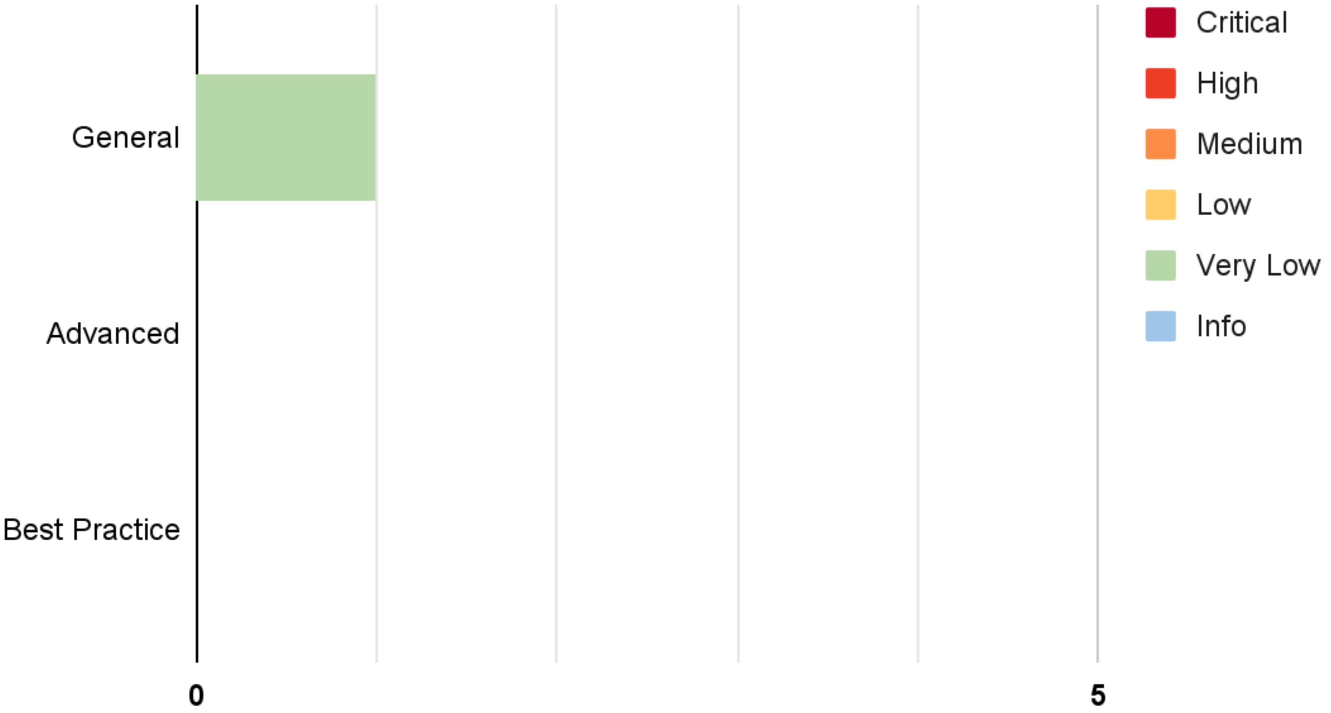
Both likelihood and impact can be categorized into three levels: **Low**, **Medium**, and **High**.

Severity is the overall risk of the issue. It can be categorized into five levels: **Very Low**, **Low**, **Medium**, **High**, and **Critical**. It is calculated from the combination of likelihood and impact factors using the matrix below. The severity of findings with no likelihood or impact would be categorized as **Info**.

Likelihood Impact	Low	Medium	High
Low	Very Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical

4. Summary of Findings

From the assessments, Inspex has found 1 issue in three categories. The following chart shows the number of the issues categorized into three categories: **General**, **Advanced**, and **Best Practice**.



The statuses of the issues are defined as follows:

Status	Description
Resolved	The issue has been resolved and has no further complications.
Resolved *	The issue has been resolved with mitigations and clarifications. For the clarification or mitigation detail, please refer to Chapter 5.
Acknowledged	The issue's risk has been acknowledged and accepted.
No Security Impact	The best practice recommendation has been acknowledged.

The information and status of each issue can be found in the following table:

ID	Title	Category	Severity	Status
IDX-001	Outdated Compiler Version	General	**Very Low**	Resolved

* The mitigations or clarifications by Baryon Network can be found in Chapter 5.

5. Detailed Findings Information

5.1 Outdated Compiler Version

ID	IDX-001
Target	BaryonERC20 BaryonPair BaryonFactory BaryonRouter
Category	General Smart Contract Vulnerability
CWE	CWE-1104: Use of Unmaintained Third Party Components
Risk	**Severity:** Very Low **Impact:** Low From the list of known Solidity bugs, direct impact cannot be caused from those bugs themselves. **Likelihood:** Low From the list of known Solidity bugs, it is very unlikely that those bugs would affect these smart contracts.
Status	Resolved Baryon Network team has resolved this issue as suggested in commit `c717b1e70dcc2010201a49524a6b940904f8d0cf` by applying the new Solidity compiler version for the contracts that use the outdated Solidity compiler version.

5.1.1 Description

The Solidity compiler versions specified in the smart contracts were outdated. These versions have publicly known inherent bugs[2] that may potentially be used to cause damage to the smart contracts or the users of the smart contracts.

The following contracts are using the outdated compiler:

Contract	Solidity Compiler Version
BaryonERC20	0.5.16
BaryonPair	0.5.16
BaryonFactory	0.5.16
BaryonRouter	0.6.6

5.1.2 Remediation

Inspex suggests upgrading the Solidity compiler to the latest stable version[3]. During the audit activity, the latest stable versions of Solidity compiler in major 0.5 (0.5.x) is 0.5.17 and major 0.6 (0.6.x) is 0.6.12.

Please note that for the `BaryonRouter` contract, some dependencies require a specific compiler version, please verify its compatibility before upgrading it.

6. Appendix

6.1. About Inspex

CYBERSECURITY
PROFESSIONAL
SERVICE

Inspex is formed by a team of cybersecurity experts highly experienced in various fields of cybersecurity. We provide blockchain and smart contract professional services at the highest quality to enhance the security of our clients and the overall blockchain ecosystem.

Follow Us On:

Website	https://inspex.co
Twitter	@InspexCo
Facebook	https://www.facebook.com/InspexCo
Telegram	@inspex_announcement

6.2. References

[1] "OWASP Risk Rating Methodology." [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology. [Accessed: 08-May-2021]

[2] "Ethereum - known issues" [Online]. Available: https://docs.soliditylang.org/en/latest/bugs.html. [Accessed: 06-January-2022]

[3] "Ethereum - releases" [Online]. Available: https://github.com/ethereum/solidity/releases. [Accessed: 06-January-2022]

inspex

CYBERSECURITY PROFESSIONAL SERVICE