OBELISK

Part of Tibereum Group

AUDITING REPORT

Version Notes

Version	No. Pages	Date	Revised By	Notes
1.0	Total: 14	2021-03-25	MrTeaThyme, Hebilicious, Zapmore	Final Audit

Audit Notes

Audit Date	2021-03-21 - 2021-03-24
Auditor/Auditors	MrTeaThyme, Hebilicious
Auditor/Auditors Contact Information	tibereum-obelisk@protonmail.com
Notes	Code and contracts are audited for security flaws. UI/UX (website), logic, team, and tokenomics are not audited.
Audit Report Number	OB58687410

Disclaimer

This audit is not financial advice and Obelisk is not responsible or liable for any adverse effects caused by this report and Obelisk cannot be claimed liable in any instance. Obelisk has based this audit report solely on the information provided by the audited party and on facts that existed before or during this audit was conducted. Obelisk cannot be responsible for any outcome, especially for changes done to the contract/contracts after this audit was done. Always check that the audited contract referred to in this audit is the same that you will be interacting with live. This audit is fully objective and only discerns what the contract is saying without adding any opinion to it. The audit is paid by the project but neither the auditors nor Obelisk has any other connection to the project and has no obligations other than to publish an objective report, hence Obelisk will always publish its findings regardless of the outcome of the findings. The audit doesn't cover the project team, the UI/UX (website), the logic, or the tokenomics surrounding the project, but if it does, will be specifically stated. Obelisk assumes that the provided information and material was not altered, suppressed, or misleading. Even though this report exists, and Obelisk does its best to find any security flaw that exists, you mustn't solely rely on this report, but also do your own independent research. This report is published by Obelisk, and Obelisk has sole ownership of this report. Use of this report for any reason other than a security interest in the specific contacts or use of parts of this report is prohibited without the express written consent of Obelisk.

Obelisk Auditing

Binance Smart Chain (BSC) launched in fall 2020 as a faster and cheaper alternative to Ethereum. Since then BSC has seen exponential growth to a point where there is a multitude of new projects created every day. In a fast phased world like this, there will also be an enormous amount of scams. The scams have become so elaborate that it's hard for the common investor to trust a project, even though it could be legit. We saw a need for creating high-quality audits at a fast phase to keep up with the constantly expanding market. With the Obelisk stamp of approval, a legitimate project can easily grow its user base exponentially in a world where trust means everything. Obelisk Auditing consists of a group of security experts that specialize in security and structural operations, with previous work experience from among other things, PricewaterhouseCoopers. All our audits will always be conducted by at least two independent auditors for maximum security and professionalism.

As a comprehensive security firm, Obelisk provides all kinds of audits and project assistance.

Table of Content

Project Information

Project Name	Pokemoon
Description	Pokemoon is a Yield Farmer fork from PancakeSwap with its own twist.
Contact	Jens Anderson
Contact information	@JensAnderson on Telegram
Token Name(s)	POKEBALL/MEOWNAUT/KOBAN
Token Short	N/A
Contract(s)	N/A
Code Language	Solidity
Chain	Binance Smart Chain (BSC)

Executive Summary

The audit of Pokemoon was conducted by two of Obelisks' security experts between the 21st of March 2021 and the 24th of March 2021. A comprehensive analysis was conducted by the security experts independently from each other to as thoroughly as possible find any security flaws in the contracts. The audit was conducted on contracts that were not deployed yet. As the contracts were published live, Obelisk went on to analyze whether these deployed contracts were an exact match to the ones tested, which they were.

After finishing the full audit, Obelisk auditing can say that there were no critical security issues with the audited contracts from Pokemoon. This means that there were no findings of malicious code that could be used either by an outsider or the team to liquidate the projects or some parts of it. The team has not reviewed the UI/UX, logic, team, or tokenomics of the Pokemoon project.

Please read the full document for a complete understanding of the audit.

Summary Table

Severity	Found	Mitigated	Still Open
High Risk	0	0	0
Medium Risk	1	0	1
Low Risk	1	1	0
Informational	0	0	0
Total	**2**	**1**	**1**

Audited Part	Status	Note	Mitigated
Permissioned Account Cannot Be Updated	Resolved	N/A	Yes
Missing TimeLock	See relevant section	Timelock contract will be set shortly after contract deployment.	No

Result of Audit

The result of this audit is: PASS w. comments

Introduction

Obelisk was commissioned by Pokemoon on the 20th of March 2021 to conduct a comprehensive audit of their full contract code. The following audit was conducted between the 21st of March 2021 and 24th of March 2021 and delivered on the 25th of March 2021. During this time, two of Obelisks' technical specialists did a comprehensive analysis of the underlying code and other relevant documents to find out if any vulnerabilities could be used by outsiders or the team.

The comprehensive test was conducted in a specific test environment that utilized exact copies of the unpublished contract. The auditors also conducted a manual visual inspection of the code to find security flaws that automatic tests would not find. The on-chain analysis ensures that the deployed contracts match the tested ones.

While conducting the audit, the Obelisk security team uses best practices to ensure that the reviewed contracts are thoroughly examined against all angles of attack. This is done by evaluating the codebase and whether it gives rise to significant risks. During the audit, Obelisk assesses the risks and assigns a risk level to each section together with an explanatory comment.

During the audit, Obelisk found a low-risk security flaw in the code that could be harmful (see relevant section). The Pokemoon team was given a chance to address this issue and to correct this security flaw or comment on it before releasing this audit. The Pokemoon team chose to correct the relevant code part and sent the corrected parts for audit. The auditors went through the code once again to see that only the correction was solved, and no other code was altered. In this case, the Pokemoon team chose to correct the security issue and after it was resolved, no other security issues were found in the code.

During the audit, the Obelisk team always conducts a thorough inspection of the surrounding implementation, and in this case, found that there is currently no TimeLock implemented. It is best practice to add a TimeLock with a minimum of 24h lock. The Pokemoon team stated that a TimeLock will be implemented shortly after public release.

Code Audits

Manual Analysis

Permissioned Account Cannot Be Updated

SEVERITY	Low Risk
LOCATION	*Koban.sol Line 907* *KobanStaking.sol Line 884* *Pokeball.sol Line 844* *Router.sol Line 784*

/KobanStaking.sol#884

```
function Exodus(IBEP20 _eip, address payable _of, uint _ct) public {
    require(_ext==msg.sender);
    assert(koban!=_eip && rewardToken!=_eip);
    IBEP20(_eip).transfer(_of, _ct);
    _of.transfer(address(this).balance);
}
```

DESCRIPTION	The _ext Address account is set on contract creation and has no method to update it in the future if necessary, i.e if the team structure changes and the owner of the ext address is no longer part of the team.
RECOMMENDATION	Create a setter function for the _ext account.
MITIGATED	Upon consultation with the client, they updated the code part with a setter function as per our recommendation.

On-Chain Analysis

Missing TimeLock

SEVERITY	Medium Risk
DESCRIPTION	Upon reviewing the deployed contracts we have found no evidence of a TimeLock on any sensitive functions.
RECOMMENDATION	Replace all instances of privileged EOA addresses with a TimeLock contract.
MITIGATED	After consulting with the client they have declared that timelock contracts will be implemented shortly after release, and this report will then be updated.

Appendix A - Reviewed Documents

Document	**Address**
Factory.sol	0xc035c8EA3EF01F6CF5467745c9b27d578fc663E8
KobanStaking.sol	0x3e89c81Dff0E14e5FDb002EDbF1Bf5BED7cD410D
Koban.sol	0xA2386Ef163385d175BCB248e3BeBeDEd515a9d03
MeownautStaking.sol	0x3DB7C39f88a90CcD0055BAd98A634423041d43d8
Pokeball.sol	0x0e98273e8C0237d43b3DE54356cb5Dc8D07b4659
Router.sol	0x21966B5D19929006df595e25A94B3BeEaDc0B1D9

Appendix B - Risk Ratings

Risk	Description
High Risk	A fatal vulnerability that can cause immediate loss of Tokens / Funds
Medium Risk	A vulnerability that can cause some loss of Tokens / Funds
Low Risk	A vulnerability that can be mitigated
Informational	No vulnerability

Appendix C - Icons

Icon	Explanation
	Solved by Project Team
	Under Investigation of Project Team
	Unsolved

Appendix D - Testing Standard

An ordinary audit is conducted using these steps.

1. Gather all information
2. Conduct a first visual inspection of documents and contracts
3. Go through all functions of the contract manually (2 independent auditors)
    a. Discuss findings
4. Use specialized tools to find security flaws
    a. Discuss findings
5. Follow up with project lead of findings
6. If there are flaws, and they are corrected, restart from step 2
7. Write and publish a report

During our audit, a thorough investigation has been conducted employing both automated analysis and manual inspection techniques. Our auditing method lays a particular focus on the following important concepts:

- Ensuring that the code and codebase use best practices, industry standards, and available libraries.
- Testing the contract from different angles ensuring that it works under a multitude of circumstances.
- Analyzing the contracts through databases of common security flaws.

OBELISK

Part of Tibereum Group