SAFETIN AUDIT

OCTAPLEX

October 9th, 2021

TABLE OF CONTENTS

AUDIT SUMMARY

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

A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and Testnet Deployment techniques. 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
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
- Through line-by-line manual review of the entire codebase by industry expert

AUDIT OVERVIEW

VULNERABILITY SUMMARY

The Octaplex Protocol is a decentralized finance (DeFi) token deployed on the Binance smart chain (BSC).

Octaplex mainly employs three features in its protocol : flexible reward for holders, auto buy-back and marketing - admins fee :

Each Octaplex transaction is taxed 10% fees of the transaction amount. 4% is sold to be redistributed as a reward to the holders in BNB, ETH, BUSD, MATIC, ADA, BTCB and/or PLX (each user can choose his rewards). 4% is sold and accumulated internally until a sufficient amount of capital has been amassed to perform a buy-back. When this number is reached, the total BNBs accumulated are used to buy PLX. 1% is sold and used for marketing, 0.6% is sold and distributed to the admins, and 0.4% is sold and distributed to the moderators.

PRIVILEGED FUNCTIONS

The contract contains the following privileged functions that are restricted by onlyAdmin or onlyMain modifiers. They are used to modify the contract configurations and address attributes. We grouped these functions below :

OWNERSHIP MANAGEMENT

- setMarketingOwnership
- setWorkHelper
- addtoAdminList
- setMainWallet

REWARDS MANAGEMENT

- AddTokentoPayoutList
- EditPayoutList
- StartRewardCalculation
- ExcludefromTax
- UndoExcludefromTax
- setAutoCalcRewards
- swapTaxTokenForBNB
- addBNBtoHolderPot
- setPromotedRewardTokenoftheWeek
- DistributeRewards

- sendAirdrop

LIQUIDITY MANAGEMENT

- addLiquidityFromContract

OTHERS

- setNperTransfer
- StartLaunch
- ToggleTransfers
- addBNBtoGasPot
- burnbeforeLaunch

AUDIT FINDINGS

1 | Risk to run out of gas in _PayTeam

Description

There is no limit to the number of admins in the AdminList which means that if a malicious administrator adds too many admins/mods to the AdminList/ModList, the for loop could ask too much computation and the _PayTeam function could run out of gas.

2 | Third-party dependencies

Description

The contract is serving as the underlying entity to interact with third party PANCAKESWAP protocols. The scope of the audit would treat those third party entities as black boxes and assume it's functional correctness. However in the real world, third parties may be compromised that led to assets lost or stolen.

We understand that the business logic of the Octaplex Network requires the interaction PancakeSwap protocol for adding liquidity to PLX/BNB pool and swap tokens.

Recommendation

We encourage the team to constantly monitor the statuses of
those third parties to mitigate the side effects when unexpected activities are observed.

CONCLUSION

No major issue has been found in the Octaplex Network smart-contract. The two findings we reported are low severity issues, and are common to the majority of rewards smart-contracts.

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement.

This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement.

This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without Safetin's prior written consent.This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is 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 Safetin to perform a security assessment.

This report 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. This report should not be used in any way

Safetin security assessment to make decisions around investment or involvement with any particular project.

This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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. Safetin's position is that each company and individual are responsible for their own due diligence and continuous security. Safetin'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 fun.