SAFETIN AUDIT

DEGEM

October 9th, 2021

TABLE OF CONTENTS

I. SUMMARY
II. OVERVIEW
III. FINDINGS
IV. DISCLAIMER

AUDIT SUMMARY

This report has been prepared for Degem to discover issues and vulnerabilities in the source code of the Degem 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 Degem 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

UNDERSTANDING

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

Degem employs two features in its protocol : static project fee as well as an LP acquisition mechanism. Those features work as follow :

Each Degem transaction is taxed 7% fees of the transaction amount. 5% is distributed to a team wallet (60% of the funds are used for development and the remaining for marketing) whilst the other 2% is accumulated internally until a sufficient amount of capital has been amassed to perform an LP acquisition. When this number is reached, the total tokens accumulated are split with half being converted to BNB and the total being supplied to the PANCAKESWAP contract as liquidity.

PRIVILEGED FUNCTIONS

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

OWNERSHIP MANAGEMENT

- renounceOwnership
- transferOwnership
- lock

ACCOUNTS MANAGEMENT

- excludeFromReward
- includeInReward
- excludeFromFee
- includeInFee
- setMarketingWallet

TAXES MANAGEMENT

- SetTaxFeePercent
- includeInFee

LIQUIDITY MANAGEMENT

- SetNumTokensSellToAddToLiquidity
- SetSwapAndLiquifyEnabled
- setRouterAddress

TRANSACTION MANAGEMENT

- SetMaxTxPercent
- buyDegemWithLeftoverBNB
- getMaxTxAmount

AUDIT FINDINGS

1 | createPair in setRouterAddress

Description

The setRouterAddress function tries to create a new Degem / WBNB pair using the createPair method, but there is no guarantee that the new router will understand this method and thus be able to create the pair - although it is very likely that a version 3 of PancakeSwap will contain such a method, it would have been better to be able to pass the method to be called as an argument.

2 | taxFee is implemented but never used

Description

The taxFee is implemented and called in several transfer functions, however it is set to 0 and nothing seems to speak in the project about a potential activation of this tax (which would be a reflection tax), which leads to a slight waste of gas.

3 | Reflection is implemented but never used

Description

The contract is built on top of SafeMoon's, so it contains all of SafeMoon's reflection/rebase module, however since the reflection fee is zero, it doesn't make sense, and is another waste of gas.

4 | getMaxTxAmount is only callable by owner

Description

This is not a big deal at all, but it does seem strange and inconvenient. Because of the modifier onlyOwner, the only address able to call this function is the owner while it's an informational function.

5 | 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 Degem Protocol requires the interaction PancakeSwap protocol for adding liquidity to Degem/BNB pool and swap tokens.

Recommandation

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 Degem smart- contract. The findings we reported are low severity issues, and are common to the majority of rewards smart - contracts. The overall security of the smart-contract is almost perfect as it's using an already audited code base (SafeMoon code base).

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.