DEFIMOON

be secure

Smart Contract Audit Report

August, 2022

PPToken

DEFIMOON PROJECT

Audit and
Development

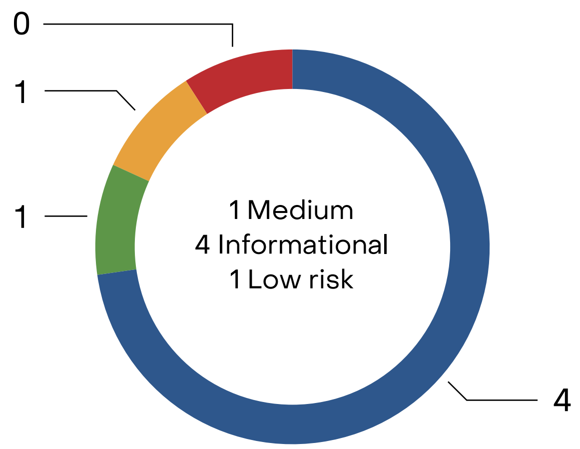
CONTACTS

https://defimoon.org
audit@defimoon.org
defimoon_org
defimoonorg
defimoon
defimoonorg

August 18th 2022
This audit report was prepared by Defimoon for PPToken

Audit information

Type	BEP-20 Token
Auditor	Aleksey Zhelyabin
Approved by	Cyrill Minyaev, Artur Makhnach
Audited contract	0xEB3e9abc909A9ddA22f4EfD2DeA7F071252E4554
Timeline	17th - 18th August 2022
Languages	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Manual Review
Chain	BSC mainnet



▶	High Risk	A fatal vulnerability that can cause the loss of all Tokens / Funds.
▶	Medium Risk	A vulnerability that can cause the loss of some Tokens / Funds.
▶	Low Risk	A vulnerability which can cause the loss of protocol functionality.
▶	Informational	Non-security issues such as functionality, style, and convention.

Check List

✅ No mint function found, owner cannot mint tokens after initial deploy

❌ Owner sets max tx amount in initialize function and it is possible to set any tx amount via function updateMaxSellTransaction().

```
_maxSellTransaction = 1_000_000 * 10**decimals(); // 1M $PPTK
```

```
function updateMaxSellTransaction(uint256 amount) external onlyOwner {
    require(
        _maxSellTransaction != amount,
        "PPToken: Max sell transaction is already the value of 'amount'"
    );

    _maxSellTransaction = amount;

    emit MaxSellTransactionUpdated(amount);
}
```

❌ Owner can set any fees via the following functions:

- updateBuyFees()
- updateLiquidityBuyFees()
- updateTeamBuyFees()
- updateMarketingBuyFees()
- updateChestBuyFees()
- updateKsosBuyFees()
- updateSellFees()
- updateLiquiditySellFees()
- updateTeamSellFees()
- updateMarketingSellFees()
- updateChestSellFees()
- updateKsosSellFees()

✅ Owner can't pause trading

❌ Owner can blacklist wallets via function:

```
function blacklistAddress(address account, bool value) external onlyOwner {
    _isBlacklisted[account] = value;
}
```

Disclaimer

This audit is not financial, investment, or any other kind of advice and could be used for informational purposes only. This report is not a substitute for doing your own research and due diligence should always be paid in full to any project. Defimoon is not responsible or liable for any loss, damage, or otherwise caused by reliance on this report for any purpose. Defimoon has based this audit report solely on the information provided by the audited party and on facts that existed before or during the audit being conducted. Defimoon is not responsible for any outcome, including changes done to the contract/contracts after the audit was published. This audit is fully objective and only discerns what the contract is saying without adding any opinion to it. Defimoon has no connection to the project other than the conduction of this audit and has no obligations other than to publish an objective report. Defimoon will always publish its findings regardless of the outcome of the findings. The audit only covers the subject areas detailed in this report and unless specifically stated, nothing else has been audited. Defimoon assumes that the provided information and materials were not altered, suppressed, or misleading. This report is published by Defimoon, and Defimoon has sole ownership of this report. Use of this report for any reason other than for informational purposes on the subjects reviewed in this report including the use of any part of this report is prohibited without the express written consent of Defimoon. In instances where an auditor or team member has a personal connection with the audited project, that auditor or team member will be excluded from viewing or impacting any internal communication regarding the specific audit.

Audit Information

Defimoon utilizes both manual and automated auditing approach to cover the most ground possible. We begin with generic static analysis automated tools to quickly assess the overall state of the contract. We then move to a comprehensive manual code analysis, which enables us to find security flaws that automated tools would miss. Finally, we conduct an extensive unit testing to make sure contract behaves as expected under stress conditions.

In our decision making process we rely on finding located via the manual code inspection and testing. If an automated tool raises a possible vulnerability, we always investigate it further manually to make a final verdict. All our tests are run in a special test environment which matches the "real world" situations and we utilize exact copies of the published or provided contracts.

While conducting the audit, the Defimoon 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, Defimoon assesses the risks and assigns a risk level to each section together with an explanatory comment.

Audit overview

No critical issues were found, but there are some recommendations, that can be considered by team to improve readability, security and make the code more clear.

The proxy contract was checked and no deviations from the standard OpenZeppelin implementation were revealed.

Defimoon only audited that PPToken contract and did not audit the contracts outside of the BEP20 directory.

Summary of findings

ID	Description	Severity
DFM-1	Upgradeable contract does not protect its initialize function	Medium
DFM-2	Greedy Contract	Low risk
DFM-3	Unlocked pragma	Informational
DFM-4	Too recent version of pragma	Informational
DFM-5	Allowance Double-Spend Exploit	Informational
DFM-6	Different pragma directives are used	Informational

Application security checklist

Compiler errors	Passed
Possible delays in data delivery	Passed
Timestamp dependence	Passed
Integer Overflow and Underflow	Passed
Race Conditions and Reentrancy	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Private user data leaks	Passed
Malicious Events Log	Passed
Scoping and Declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Design Logic	Passed
Cross-function race conditions	Passed
Safe OpenZeppelin contracts and implementations usage	Unresolved
Front Running	Passed
Solidity version not specified or too old	Unresolved
Function input parameters lack of check	Passed
Function access control lacks management	Passed
Critical operation lacks event log	Passed
Human/contract checks bypass	Passed
Fallback function misuse	Unresolved
Logical vulnerability	Passed
Visibility not explicitly declared	Passed
Variable storage location not explicitly declared	Passed
High gas consumption / «Out of Gas» attack	Passed

Findings

DFM-1 «Upgradeable contract does not protect its initialize function»

Severity: Medium

Description: Upgradeable contracts does not protect its initiliaze functions.

Recommendation: Invoke `_disableInitializers()` on the constructor of upgradeable contracts (OpenZeppelin Doc) to avoid leaving the implementation contract uninitialized.

DFM-2 «Greedy Contract»

Severity: Low risk

Description: A greedy contract is a contract that can receive ether which can never be redeemed.

Recommendation: In accordance with best practices, to prevent tokens being accidentally stuck in the BEP20 contract itself, it is recommended to prevent the transferal of tokens to the contracts address. This can be achieved, by i.e. adding require statements to transfer functions, similar to `require(to != address(this));`.

DFM-3 «Unlocked pragma»

Severity: Informational

Related issue: SWC-103

Description: Every Solidity file specifies in the header a version number of the format `pragma solidity (^)0.8.*`. The caret (^) before the version number implies an unlocked pragma, meaning that the compiler will use the specified version *and above*, hence the term "unlocked".

Recommendation: For consistency and to prevent unexpected behavior in the future, we recommend to remove the caret to lock the file onto a specific Solidity version.

DFM-4 «Too recent pragma version»

Severity: Informational

Description: `pragma ^0.8.16` - version too recent to be trusted.

Recommendation: Consider deploying with `0.6.12/0.7.6/0.8.7`

DFM-5 «Allowance Double-Spend Exploit»

Severity: Informational

Description: As it presently is constructed, the contract is vulnerable to the allowance double-spend exploit, as with other BEP20 tokens.

Exploit Scenario:

1. Alice allows Bob to transfer N amount of Alice's tokens (N>0) by calling the `approve()` method on Token smart contract (passing Bob's address and N as method arguments)
2. After some time, Alice decides to change from N to M (M>0) the number of Alice's tokens Bob is allowed to transfer, so she calls the `approve()` method again, this time passing Bob's address and M as method arguments.
3. Bob notices Alice's second transaction before it was mined and quickly sends another transaction that calls the `transferFrom()` method to transfer Alice's tokens somewhere.
4. If Bob's transaction will be executed before Alice's transaction, then Bob will successfully transfer N Alice's tokens and will gain an ability to transfer another M tokens.
5. Before Alice notices any irregularities, Bob calls `transferFrom()` method again, this time to transfer M Alice's tokens.

DFM-6 «Different pragma directives are used»

Severity: Informational

Description: `solc` frequently releases new compiler versions. Using an old version prevents access to new Solidity security checks. We also recommend avoiding complex `pragma` statement.

Recommendation: Deploy with any of the following Solidity versions:

- `0.5.16 - 0.5.17`
- `0.6.11 - 0.6.12`
- `0.7.5 - 0.7.6`
- `0.8.4 - 0.8.7`

  Use a simple pragma version that allows any of these versions. Consider using the latest version of Solidity for testing.

Automated Analyses

Slither

Slither report 98 results. These results were either related to code from dependencies, false positives or have been integrated in the findings or best practices of this report.

Adherence to Best Practices

- More comments should be added for better readability of the code. Using NatSpec format.

Methodology

Manual Code Review

We prefer to work with a transparent process and make our reviews a collaborative effort. The goal of our security audits is to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Vulnerability Analysis

Our audit techniques include manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high-level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, review open issue tickets, and investigate details other than the implementation.

Documenting Results

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system to make a final decision.

Suggested Solutions

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Appendix A — Finding Statuses

Mitigated	The finding was resolved by other methods such as revoking contract ownership or updating the code to minimize the effect of the finding
Acknowledged	Project team is made aware of the finding
Open	The finding was not addressed