AUDIT REPORT

PROJECT : Polysec.finance

1. Introduction

1. About Project

Project Name: Polysec Finance

The contract is: 0xB0d5300dC7230A137D4D738DA0113EB0E00a571d

Standard: ERC20 on Polygon Mainnet.

2. Disclaimer

.

This audit is only to the Smart-Contract code at the specified address.: https://polygonscan.com/address/0xb0d5300dc7230a137d4d738da0113eb0e00a571d#code

Solidikey is a 3rd party auditing company that works on audits based on client requests. And as a professional auditing firm, we check on the contract for any vulnerabilities, backdoors, and/or scam scripts.

Therefore:

- We are not financial advisors nor do we partner with the contract owners
- Operations and website administration is fully on the client's side.
- We do not have influence over client operations, which can lead to website changes, withdrawal function closes, etc. One always has the option to do this through the contract.
- Any concerns about the project themselves need to be raised directly to the project owners and not through Solidikey.
- Investors are not in any way obliged, coerced, or influenced to invest in projects audited by Solidikey.
- We are not responsible for your funds or guarantee you profits.

2. Findings

1. **CRITICAL ISSUES (critical, high severity): 0**

Critical and harmful access for owners, user block ability, Bugs, and vulnerabilities that enable theft of funds, lock access to funds without possibility to restore it or lead to any other loss of funds to be transferred to any party.

2. **ERRORS, BUGS AND WARNINGS (medium, low severity): 0**

Bugs can negatively affect the usability of a program, errors that can trigger a contract failure, Lack of necessary security precautions, other warnings for owners and users, warning codes that are valid code but the compiler thinks are suspicious.

3. **OPTIMIZATION (low severity): 1**

Methods to decrease the cost of transactions in Smart-Contract.

4. **RECOMMENDATIONS (very low severity): 0**

Hint and tips to improve contract functionality and trustworthiness.

5. **Data Processing Errors: 0**

Weaknesses in this category are typically found in functionality that processes data. Data processing is the manipulation of input to retrieve or save information. The software filters data in a way that causes it to be reduced or "collapsed" into an unsafe value that violates an expected security property. The software does not properly handle when the expected number of values for parameters, fields, or arguments is not provided in input, or if those values are undefined.

No related vulnerabilities in smart contract code.

6. **Bad coding practices: 0**

Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. These weaknesses do not directly introduce a vulnerability, but indicate that the product has not been carefully developed or maintained. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

No related vulnerabilities in smart contract code.

3. Optimization suggestions

1. Loop on the dynamic variable (low severity).

If the user gets more parallel deposits his withdrawal transaction fee will cost more because the loop on the dynamic variable is used in the ‘withdraw’ function.

In case of the GAS limit of exceeding the size of transaction withdraw is not possible.

Note:

This comment is relevant only if a user creates an excessive number of parallel deposits (more than 100).

4. Conclusion

In the **Polysec** Smart-Contract were found no vulnerabilities, no backdoors, and **no scam scripts**.

The code was tested with compatible compilers and simulate manually reviewed for all commonly known and specific vulnerabilities.
So, Polysec Smart-Contract is safe for use in the Polygon Mainnet network.

5. Independent description of Smart Contract functionalities

The **Polysec** smart contract provides the opportunity to invest any amount in MATIC (from 10 MATIC) in the contract and get 112% to 367% return on investment in 14 to 35 days if the contract balance has enough funds for payment.

- Dividends are paid from deposits of users.

- All dividends are calculated at the moment of request and available for withdrawal anytime or after deposit finished time based on plans

- Each subsequent Deposit is kept separately in the contract, in order to maintain the payment amount for each Deposit.

Launch Date: Sat Jun 30 2021 13:39:00 GMT+0000

1. **Contract Owners Fee:**

Dev Fee: 6%

Pro Fee: 6%.

2. **Eight INVESTMENT PLANS**

Plans	Total Return	Daily Profit	Days	Withdraw Time
1	112%	8%	14	Any Time
2	136%	6.5%	21	Any Time
3	154%	5.5%	28	Any Time
4	158%	4.5%	35	Any Time
5	193%	13.8%	14	End of Plan
6	275%	13.1%	21	End of Plan

7	347%	12.4%	28	End of Plan
8	367%	10.5 %	35	End of Plan

3. Float Plan

Plans return are float and daily profit for a new deposit will increase by 0.3% daily.

4. Termination/Force Withdraw

Plan 5-8 can be terminated anytime and get 50% deposit back before the end of plan, 1-4 are not allowed to terminate

5. Referral System (Match Bonus)

The contract pays an 6% referral commission in single level.

Notes: Referral should be an active user; it means referral address has at least one deposit.

06/26/2021

If you are interested in auditing/developing a smart contract, please contact us here.
Our Website : https://solidikey.us