MoneyToad

Disclaimer

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed. By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SECURITY NETWORK hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. No one shall have any right to rely on the report or its contents, and SECURITY NETWORK and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SECURITY NETWORK) owe no duty of care towards you or any other person, nor does SECURITY NETWORK make any warranty or representation to any person on the accuracy or completeness of the report. Except and only to the extent that it is prohibited by law, SECURITY NETWORK hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SECURITY NETWORK, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The issuance of an audit report is not a guarantee that a contract is safe. Please read the report to the end!

Audited project: MoneyToad

Decimals: 18

Address contract: 0xd2d28013E97161cb58bfD36643cC93a3E137ec37

Compiler Version: v0.8.9+commit.e5eed63a

Optimization Enabled: No with 200 runs

Contract Deployer Address: 0xdbcD34949e3c47655F1E518E0110C059EfbD5CED

Project website: https://moneytoad.app/

KYC: no

Languages: Solidity (Smart contract)

Blockchain: Binance Smart Chain

Audit Team: SECURITY NETWORK

https://securitynetwork.pro/

Audit Date: July 26, 2022

SWC Attacks

SWC ID	Title	Status
SWC-100	Function Default Visibility	PASSED
SWC-101	Integer Overflow and Underflow	PASSED
SWC-102	Outdated Compiler Version	PASSED
SWC-103	Floating Pragma	PASSED
SWC-104	Unchecked Call Return Value	PASSED
SWC-105	Unprotected Ether Withdrawal	PASSED
SWC-106	Unprotected SELFDESTRUCT Instruction	PASSED
SWC-107	Reentrancy	PASSED
SWC-108	State Variable Default Visibility	PASSED
SWC-109	Uninitialized Storage Pointer	PASSED
SWC-110	Assert Violation	PASSED
SWC-111	Use of Deprecated Solidity Functions	PASSED
SWC-112	Delegatecall to Untrusted Callee	PASSED
SWC-113	DoS with Failed Call	MEDIUM
SWC-114	Transaction Order Dependence	PASSED
SWC-115	Authorization through tx.origin	PASSED
SWC-116	Block values as a proxy for time	PASSED
SWC-117	Signature Malleability	PASSED
SWC-118	Incorrect Constructor Name	PASSED
SWC-119	Shadowing State Variables	PASSED
SWC-120	Weak Sources of Randomness from Chain Attributes	PASSED
SWC-121	Missing Protection against Signature Replay Attacks	PASSED
SWC-122	Lack of Proper Signature Verification	PASSED
SWC-123	Requirement Violation	PASSED
SWC-124	Write to Arbitrary Storage Location	PASSED
SWC-125	Incorrect Inheritance Order	PASSED
SWC-126	Insufficient Gas Griefing	PASSED
SWC-127	Arbitrary Jump with Function Type Variable	PASSED
SWC-128	DoS With Block Gas Limit	PASSED
SWC-129	Typographical Error	PASSED
SWC-130	Right-To-Left-Override control character (U+202E)	PASSED
SWC-131	Presence of unused variables	PASSED
SWC-132	Unexpected Ether balance	PASSED
SWC-133	Hash Collisions With Multiple Variable Length Arguments	PASSED
SWC-134	Message call with hardcoded gas amount	PASSED
SWC-135	Code With No Effects	PASSED
SWC-136	Unencrypted Private Data On-Chain	PASSED

Possible additional HIGH risks

№	Issue description.	Status
1	High fees	NO
2	Mint function	NO
3	Max Tx Amount	NO
4	Pause trading without limit	NO
5	Cooldown time for sell without limit	NO
6	Proxy	NO
7	Other risks	NO

TOTAL

HIGH 0

MEDIUM 1

LOW 0

Conclusion

This smart contract containt medium severity issue:

1. SWC-113. Multiple calls are executed in the same transaction.

```
payable (msg.sender).transfer(SafeMath.sub(eggValue,fee));
```

This call is executed following another call within the same transaction. It is possible that the call never gets executed if a prior call fails permanently. This might be caused intentionally by a malicious callee. If possible, refactor the code such that each transaction only executes one external call or make sure that all callees can be trusted (i.e. they're part of your own codebase).


SN
SECURITY
NETWORK