Telescr.in

Audit of smart contracts Plastic Token

revision 5 dated 27.05.2021

Telescr.in

Summary

Brief information

Project: Plastic Token
Network: BNB
Compiler version: 0.5.12
Optimization: Enabled
Audit date: 27.05.2021

Information

The contract code was reviewed and analysed for vulnerabilities, logical errors and developer exit scams possibilities. This work was carried out concerning the project source code and documentation provided by the customer.

Customer provided project whitepaper, the audit was made based on Chapter 5 - Tokenomics of provided document.

General conclusion

As a result of the audit, no errors were found that affect the security of users' funds on the contract. No obvious signs of an exit scam were found. No backdoors found either. This is a set of contracts, that are tied together. Tokensale contract is the basic for PLAS token distribution.

Telescr.in guarantees the plastic finance contract security and performance.

Liability disclaimer

The telescr.in team within this audit framework is not responsible for the developers or third parties' actions on the platforms associated with this project (websites, mobile applications, and so on). The audit confirms and guarantees only the smart contract correct functioning in the revision provided by the project developers.

Confirmed by digital signature

Aggregated data

The Contract analysis was performed using the following methods:

- Static analysis
  - Checking the code for common errors leading to the most common vulnerabilities
- Dynamic analysis
  - The Contract launching and carrying out the attacks various kinds to identify vulnerabilities
- Code Review

Received data

Recommendation	Type	Priority	Occurrence probability	Line of error
Unnecessary functionality	remark	low		Token.sol
Governance votes are updated only after the next block is mined	remark	low		Token.sol, 216
Angel investments are controlled outside the contract	remark	low	low	tokensale.sol, 126-141
Missing control of angel funds split	remark	low	low	tokensale.sol, 126-141
Angel investments can be made on private, pre and public sale rounds	notice	low	low	tokensale.sol, 126-141
Investors should pay attention if OPENTIME is defined	remark	low	low	tokensale.sol, 126-141
Incorrect calculation	notice	low	medium	tokensale, 236
Possible losing of tokens	warning	low	medium	tokensale.sol, 335-344
Investor notice	notice	low	N/a	tokensale.sol
Angel investor notice	notice	low	N/a	tokensale.sol

A. Errors

Not found.

B. Warnings

1. Possible losing of tokens

Incorrect calculation of tokens to withdraw. In case when not all seed tokens are sold out, those unsold tokens will be locked on contract.

C. Notice

1. Angel investments can be made on private, pre and public sale rounds

According to logic of early adoption, it should be done only on the very first round of tokensale and possibly should be locked on other rounds.

2. Incorrect calculation

WithdrawFund event will always contain 0 as BNB value. Withdraw amount is correct in both BUSD and BNB.

3. Investor notice

Before investing investor should make sure that 15.8M PLAS is transferred to contract balance

4. Angel investor notice

Current implementation of unlock periods slightly contradicts with documentation (unlocking happens 1 month earlier)

D. Remarks

1. Unnecessary functionality

Governance functionality is implemented but there is neither reflection in documentation, nor obvious signs that this functionality is needed in token, although this functionality can be utilized by external contract

2. Governance votes are updated only after the next block is mined

When votes are updated in Block X, getPriorVotes won't be able to return number of votes until the Block X+1 is mined

3. Angel investments are controlled outside the contract

Angel investments are controlled by contract owner, purchase and reckoning happen outside the contract.

4. Missing control of angel funds split

Although angel investments are split into two parts, there is no logic controlling two groups distribution in the contract. These two parts have fixed values according to documentation, but this is not covered by code.

5. Investors should pay attention if OPENTIME is defined

Investor should check if the OPENTIME is defined by calling contractInfo(). This affects time of token unlocking.

Application. Error classification

Priority	
informational	This question is not directly related to functionality but may be important to understand.
low	This question has nothing to do with security, but it can affect some behavior in unexpected ways.
medium	The problem affects some functionality but does not result in an economically significant user funds loss.
high	This issue can result in the user funds loss.
Probability	
low	It is unlikely that the system is in a state in which an error could occur or could be caused by any party.
medium	This problem may likely arise or be caused by some party.
high	It is highly likely that this problem could arise or could be exploited by some parties.

Application. Digital bytecode print

The audit was carried out for the code certain version on the compiler version 0.5.12 with the optimization enabled.

To check the contract bytecode for identity to the one that was analyzed during the audit, you must:
1. Get contract bytecode (in any block explorer)
2. Get SHA1 from bytecode string
3. Compare with reference in this report

Sha1 from bytecode:
8bd69e0216a0454af79ae7d604cb92a3289f2174 - Token.sol
3f4812e4fcc3883ed55eb9e4e61a98030ad95d2f - Tokensale.sol
Sha1 from bytecode (non-metadata):
d730affebfcd1a3b4a3e960671e6114f1805d927 - Token.sol
76595b8b73c7d9f93f86945f3bab9bc8edf5e621 - Tokensale.sol
Contract address:
0xCe34caAEe0b691F8e4098DC31CC8818A1dCcF06A - Token.sol
0x1800C25a3Ed60B41766B8EE94f40CE05A84407aB - Tokensale.sol

Check the digital print

Application. Signature of the audit report

{ "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e", "msg": "As a result of the audit, no errors were found that affect the security of users' funds on the contract. No obvious signs of an exit scam were found. No backdoors found either. This is a set of contracts, that are tied together. Tokensale contract is the basic for PLAS token distribution. Telescr.in guarantees the plastic finance contract security and performance. Sha1 of contracts - 8bd69e0216a0454af79ae7d604cb92a3289f2174 - Token.sol 3f4812e4fcc3883ed55eb9e4e61a98030ad95d2f - Tokensale.sol. Sha1 without meta of contracts - d730affebfcd1a3b4a3e960671e6114f1805d927 - Token.sol 76595b8b73c7d9f93f86945f3bab9bc8edf5e621 - Tokensale.sol. Contracts address - 0xCe34caAEe0b691F8e4098DC31CC8818A1dCcF06A - Token.sol 0x1800C25a3Ed60B41766B8EE94f40CE05A84407aB - Tokensale.sol", "sig": "0xf610bb3dbe976d47c4e42b1335a42a7a1fe4323401daf75801d7bce7e8a5962d6fb77f84bbb9840886a9b92545fbc47f63a578a215c164f2769725b62a197dbc1b", "version": "3" }

Check the signature