Audit of smart contract ANTd

revision 1 dated 09.09.2021

Summary

Brief information

Project: ANTd
Network: ETH
Compiler version: 0.8.0
Optimization: Enabled
Audit date: 09.09.2021

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 provided by the customer.

Customer provided contract source code only. We have performed only token audit, no DeFi economics was reviewed. Review was made using common sense, author may have another vision on logic and functionality correctness.

General conclusion

As a result of the audit, no errors were found that affect the security of users' tokens on the contract. No backdoors found either. No DeFi economics contract was provided so we worked only on token contract.

Telescr.in guarantee the safety and performance of the contract ANTd

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**
Hardcoded address	notice	low		953
Unused class constant	remark	low		938
Unnecesary functionality	remark	low	low	965
Unnecessary functionality	remark	low	low	937
Unnecessary import	remark	low	low	677-927
Unnecessary import	remark	low	low	62-129
Unnecessary import	remark	low	low	5-61

A. Errors

Not found.

B. Warnings

Not found.

C. Notice

1. Hardcoded address

Hardcoded address in contract constructor

D. Remarks

1. Unused class constant

Constant MINTER_ROLE defined but never used

2. Unnecesary functionality

Role transferring functionality makes no sense as having Admin role doesn't bring any benefit

3. Unnecessary functionality

Access control functionality is added to contract but there is no usages of such functionality, therefore it make no sense using this extension in token contract

4. Unnecessary import

Coming from previous remark - AccessControl functionality can be omitted and AccessControl import can be excluded

5. Unnecessary import

Strings library is used only by AccessControl class Coming from previous remark - AccessControl functionality can be omitted and String import can be excluded

6. Unnecessary import

ERC165 functionality is used only by AccessControl class Coming from previous notice - AccessControl functionality can be omitted and IERC165 and ERC165 import can be excluded

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 0.8.0 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:
3ce40b2f3a8ffcbad17f256b9bbff478ec7ef0d0

Sha1 from bytecode (non-metadata):
2cbefdead4e6d24ed521b9004112d4ea48a716bc

Contract address:
0xF85ba4a69aE05308249f19F5a25e9BE765576340

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' tokens on the contract. No backdoors found either. No DeFi
economics contract was provided so we worked only on token contract. Telescr.in guarantee the safety and performance of the contract ANTd . Sha1 of contract -
3ce40b2f3a8ffcbad17f256b9bbff478ec7ef0d0 . Sha1 without meta of contract - 2cbefdead4e6d24ed521b9004112d4ea48a716bc Contract address -
0xF85ba4a69aE05308249f19F5a25e9BE765576340",
        "sig": "0xb2e9371004d0b80f82832e4757c04b24e4ee0a8e1d5b052702b8c4115c6668ef6ea8a7b961e3b9eee673e0ba3ed34153d682416ea7f897f6a1bddd01141fa36f1c",
        "version": "3"
}
```

Telescr.in

Check the signature