TechRate

Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project:	Apr War Coin
Deployer address	0xe6a428d608e71a61aaa0ffdcd85b9c7c79be0452
Blockchain:	Binance Smart Chain
Project website:	Not provided

April, 2021

TechRate

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn’t say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: 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. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate 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. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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 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.

Background

TechRate was commissioned by Apr War Coin to perform an audit of smart contracts:

- *https://bscscan.com/address/0xdfe66db4799345becca4e5a3db417150a83fdff7#code*
- *https://bscscan.com/address/0xbaec7d13898071071Db7A6f46da8e488405Cb999#code*

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 27.04.2021.

Contract name:	Apr War Coin
Compiler version:	v0.8.0+commit.c7dfd78e
Contract address:	0xdfe66db4799345becca4e5a3db417150a83fdff7
Total supply:	0
Token ticker:	AWC
Decimals:	18
Token holders:	0
Transactions count:	0
Top 100 holders dominance:	0
Contract deployer address:	0xe6a428d608e71a61aaa0ffdcd85b9c7c79be0452
Contract’s current owner address:	0xe6a428d608e71a61aaa0ffdcd85b9c7c79be0452

Masterchef contract details for 27.04.2021.

Contract name:	MasterChef
Compiler version:	v0.8.0+commit.c7dfd78e
Contract address:	0xbaec7d13898071071Db7A6f46da8e488405Cb999
Dev address:	0xde3f03dfdf040e2e35f5e0b08f239f66ba99b247
Fee address:	0x55061b2d4359accd44880643c554c92611557c3b
AWC contract address:	0xdfe66db4799345becca4e5a3db417150a83fdff7
AWC per block:	500_000_000_000_000_000
Contract owner address:	0xe6a428d608e71a61aaa0ffdcd85b9c7c79be0452
Pool length:	1
Start block:	6992000
Total alloc point:	1
Min stake fee:	1 %
Max stake fee:	4 %

MasterChef contract Pools info:

Pool with id 0:

stakeToken *address* : 0xdFE66db4799345BecCA4E5a3db417150A83Fdff7
factor *uint256* : 20
noFees *bool* : true
totalStake *uint256* : 0
totalPower *uint256* : 0
rewardPerPower *uint256* : 0
rewardUpdateBlock *uint256* : 0
allocPoint *uint256* : 1

Issues Checking Status

№	Issue description.	Checking status
1	Compiler errors.	Passed
2	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model of the contract.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Low issues
19	Cross-function race conditions.	Passed
20	Safe Open Zeppelin contracts implementation and usage.	Passed
21	Fallback function security.	Passed

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

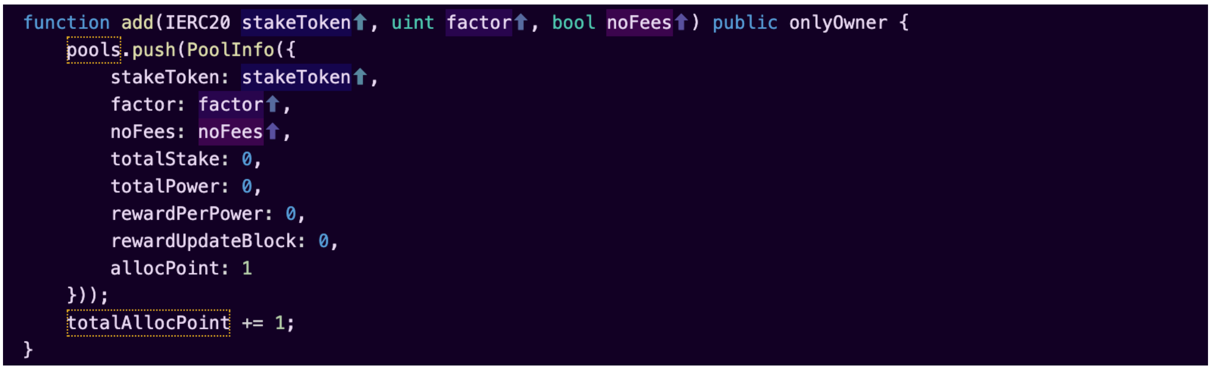
No medium severity issues found.

Low Severity Issues

1. add function issue

Issue:

If some stake token is added to the contract twice using function add, then the total amount of reward in function updatePoolReward will be incorrect.



```
function add(IERC20 stakeToken↑, uint factor↑, bool noFees↑) public onlyOwner {
    pools.push(PoolInfo({
        stakeToken: stakeToken↑,
        factor: factor↑,
        noFees: noFees↑,
        totalStake: 0,
        totalPower: 0,
        rewardPerPower: 0,
        rewardUpdateBlock: 0,
        allocPoint: 1
    }));
    totalAllocPoint += 1;
}
```

Recommendation:

Add the mapping from address to bool and check that same address will not be added twice.

Owner privileges

❏ Owner can mint any amount of tokens using function mint, until he transfers it to MasterChef contract.

❏ Owner can change the AWC per block.

❏ Owner can change the fee and dev addresses.

❏ Owner can change the bonus proxy address.

Conclusion

Smart contracts contain low severity issues and owner privileges.

Techrate note:
Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.