NOVOS

KYC & AUDIT.

Novos is an agency specializing in blockchain technology solutions, Audits, KYC / Doxx.

NOVOS

CERTIFICATE OF COMLIANCE

Smart Contract Audit by NOVOS

DACToken

Audit Passed

June 22, 2022

NOVOS

Table of Contents

NOVOS

Audit Summary

This report has been prepared for DAC Token on the Binance Chain network. Novos provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

NOVOS

Project Overview

Parameter	Result
Address	0xF5BA0856805b9B69b2a8BC89D31A473894D1f86c
Name	DACProtocol
Token Tracker	DAC
Decimals	18
Supply	1,000,000,000,000
Platform	Binance Chain
Compiler	v0.8.4+commit.c7e474f2
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0xF5BA0856805b9B69b2a8BC89D31A473894D1f86c#code
Url	https://dacprotocol.io/

Main Contract Assessed

Name	Contract	Live
DACProtocol	0xF5BA0856805b9B69b2a8BC89D31A473894D1f86c	Yes

NOVOS

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
❖ Unencrypted Private Data On-Chain	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Code With No Effects	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Message call with hardcoded gas amount	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Hash Collisions With Multiple Variable Length Arguments	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unexpected Ether balance	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Presence of unused variables	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Right-To-Left-Override control character (U+202E)	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Typographical Error	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ DoS With Block Gas Limit	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Arbitrary Jump with Function Type Variable	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Insufficient Gas Griefing	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Incorrect Inheritance Order	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Write to Arbitrary Storage Location	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Requirement Violation	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Missing Protection against Signature Replay Attacks	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Weak Sources of Randomness from Chain Attributes	✓ Complete	✓ Complete	✓ **Low / No Risk**



NOVOS

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
❖ Authorization through tx.origin	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Delegatecall to Untrusted Callee	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Use of Deprecated Solidity Functions	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Assert Violation	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Reentrancy	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unprotected SELFDESTRUCT Instruction	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unprotected Ether Withdrawal	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unchecked Call Return Value	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Outdated Compiler Version	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Integer Overflow and Underflow	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Function Default Visibility	✓ Complete	✓ Complete	✓ **Low / No Risk**



NOVOS

Contract Ownership

The contract ownership of DAC is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.
.

01

The current owner is the address 0x5960FF2E37972D627505A784A6d75297B460e2dF which can be viewed from: HERE

02

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

03

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

NOVOS

Important Notes To The Users:

01 The owner cannot stop trading.

02 The owner cannot blacklist wallets.

03 On sells there is an increase of tax based on the fees, this new tax cannot be higher than 20%.

04 Owner can enable trading but cannot pause or disable it.

05 Owner can change the maxSellTransactionAmount but it cannot be less than 10,000 tokens.

06 Owner can change the sellFeeIncreaseFactor up to 200, max sell tax is 20% (10*200/100).

07 Owner can change the claimWait for dividends between 1 hour and 24 hours.

08 Owner can change the maxWalletBalance with no constrains.

09 Owner can change and configure the dividendTracker with no constrains.

10 Owner can enable/disable the SwapAndLiquify mechanism and the BusdDividend mechainsm.

11 Owner can add/remove wallets from fee exemption and dividends.

12 Owner can change the minimum token balance needed to get dividends. No high-riskExploits /Vulnerabilities Were Found in token Source Code.

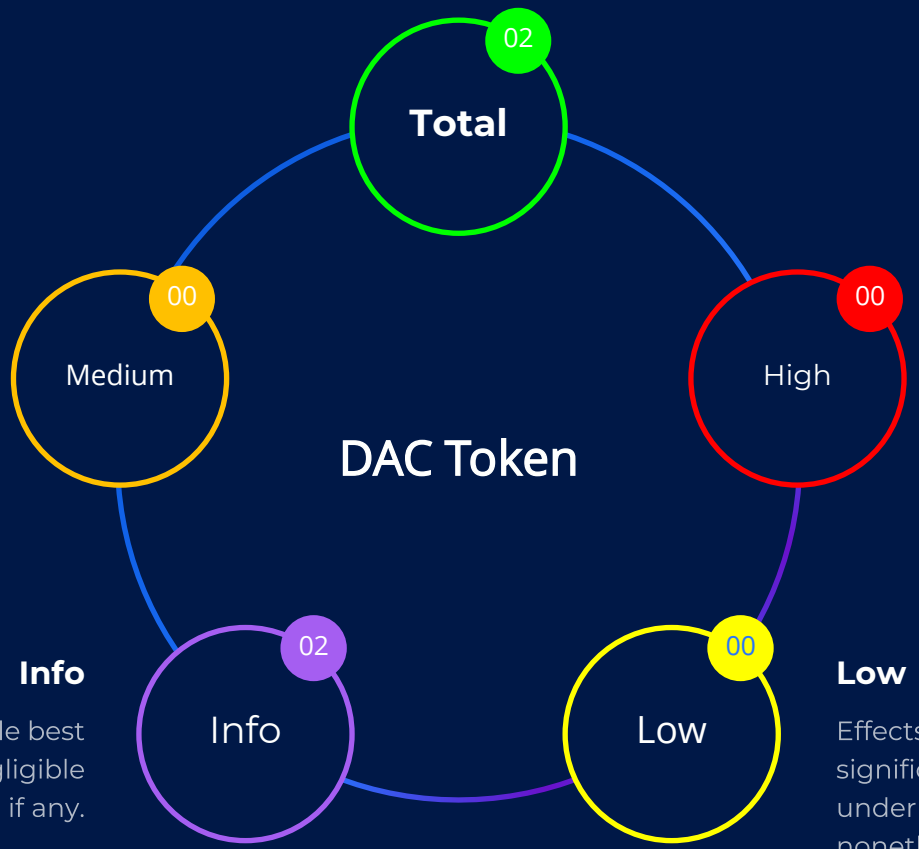
NOVOS

Technical Findings Summary

Classification of Issues

Total

What you should pay attention to



Medium

Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.

High

Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency

Info

Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

Low

Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.

NOVOS

Findings

Public function that could be declared external

ID	Severity	Contract	Function
01	Informational	DACProtocol	Functions: size, getKeyAtIndex, getIndexOfKey

Description

Gas Optimization. Public function that could be declared external

Recommendation

Public functions that are never called by the contract should be declared external to save gas.

NOVOS

Findings

Missing events arithmetic

ID	Severity	Contract	Function
02	Informational	DACProtocol	Missing events for setWalletBalance, setMaxBuyTransaction, setMaxSellTransaction, setSwapTokensAtAmount, setSellTransactionMultiplier

Description

Functions that change critical arithmetic parameters should emit an event.

Recommendation

Emit corresponding events for critical parameter changes.

NOVOS

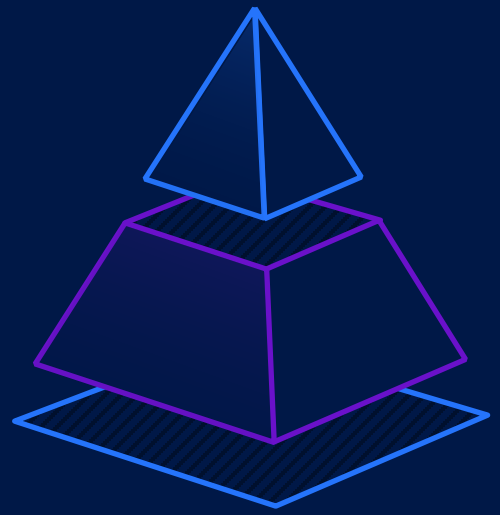
Priviliged Functions (onlyOwner & Others)

Function Name	Parameters	Visibility
✓ renounceOwnership	▪ none	▪ **external**
✓ transferOwnership	▪ address newOwner	▪ **public**
✓ prepareForPartherOrExchang eListing	▪ address_partnerOrExchangeAddress	▪ **external**
✓ setWalletBalance	▪ uint256 _maxWalletBalance	▪ **external**
✓ setMaxBuyTransaction	▪ uint256 _maxTxn	▪ **external**
✓ setMaxSellTransaction	▪ uint256 _maxTxn	▪ **external**
✓ updateBusdDividendToken	▪ address _newContract	▪ **external**
✓ updateMarketingWallet	▪ address _newWallet	▪ **external**
✓ setSwapTokensAtAmount	▪ uint256 _swapAmount	▪ **external**
✓ setSellTransactionMultiplier	▪ uint256 _multiplier	▪ **external**
✓ setTradingIsEnabled	▪ none	▪ **external**
✓ setBusdDividendEnabled	▪ bool _enabled	▪ **external**
✓ setMarketingEnabled	▪ bool _enabled	▪ **external**
✓ setSwapAndLiquifyEnabled	▪ bool _enabled	▪ **external**
✓ updatebusdDividendTracker	▪ address newAddress	▪ **external**
✓ updateUniswapV2Router	▪ address newAddress	▪ **external**

NOVOS

Priviliged Functions (onlyOwner & Others)

Function Name	Parameters	Visibility
✓ excludeFromFees	▪ address account, bool excluded	▪ **public**
✓ excludeFromDividend	▪ address account	▪ **public**
✓ setAutomatedMarketMakerP air	▪ address pair, bool value	▪ **external**
✓ updateGasForProcessing	▪ uint256 newValue	▪ **external**
✓ updateMinimumBalanceForDi vidends	▪ uint256 newMinimumBalance	▪ **external**
✓ updateClaimWait	▪ uint256 claimWait	▪ **external**
✓ processDividendTracker	▪ uint256 gas	▪ **external**



NOVOS

Statistics

Liquidity Info

Parameter	Result
Pair Address	DAC/BNB
DAC Reserves	6,716,736.8459 DAC
BNB Reserves	0.60055 BNB
Liquidity Value	$128 USD

NOVOS

Statistics

Token (DAC) Holders Info

Parameter	Result
DAC Percentage Burnt	0.3%
DAC Amount Burnt	3,000,000,000 DAC
Top 10 Percentage Own	99.9225%
Top 10 Amount Owned	999,225,000,000 DAC

NOVOS

Statistics

LP (DAC/BNB) Holders Info

Parameter	Result
DAC/BNB % Burnt	0.3%
DAC/BNB Amount Burnt	3,000,000,000 DAC/BNB
Top 10 Percentage Owned	99.9225%
Top 10 Amount Owned	999,225,000,000 DAC/BNB
Locked Tokens Percentage	0.00%

- All the data diplayed above was taken on-chain at block 18449657
- The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

NOVOS

Disclaimer

Novos has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Novos is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Novos or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by Novos is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where- is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.