Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

March, 2022

Audit Details

Audited project

Alpha Capital

Deployer address

0x01f9046b94faee17531d9c4a926834c1454d63f3

Client contacts:

Alpha Capital team

Blockchain

Ethereum

Project website:

https://alpha-cap.io/

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 Alpha Capital to perform an audit of smart contracts:

https://etherscan.io/address/0xd5a98e77d1feb091344096301ea336a5c07a6a41#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.

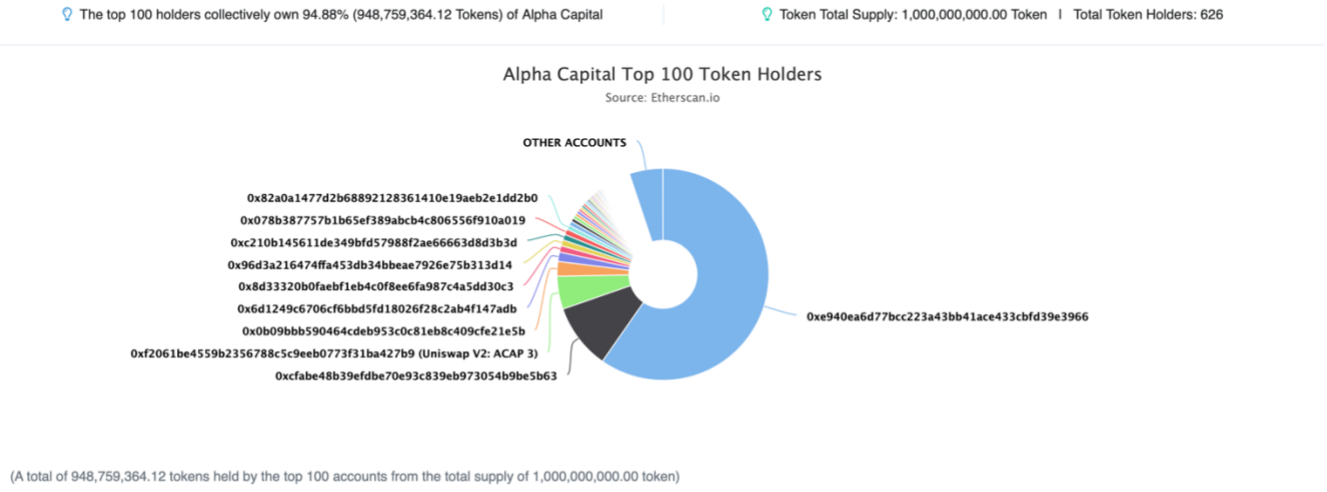
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 07.03.2022

Contract name	Alpha Capital
Contract address	0xd5A98E77d1fEB091344096301Ea336a5C07a6A41
Total supply	1,000,000,000
Token ticker	ACAP
Decimals	18
Token holders	626
Transactions count	2,031
Top 100 holders dominance	94.88%
Marketing rate	2
Reflect rate	4
Treasury rate	9
Treasury wallet	0xf914bbdff49fd4ba1a1cbfc740e0d60a8674f438
Contract deployer address	0x01f9046b94faee17531d9c4a926834c1454d63f3
Contract’s current owner address	0x01f9046b94faee17531d9c4a926834c1454d63f3

Alpha Capital Token Distribution



The top 100 holders collectively own 94.88% (948,759,364.12 Tokens) of Alpha Capital

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 626

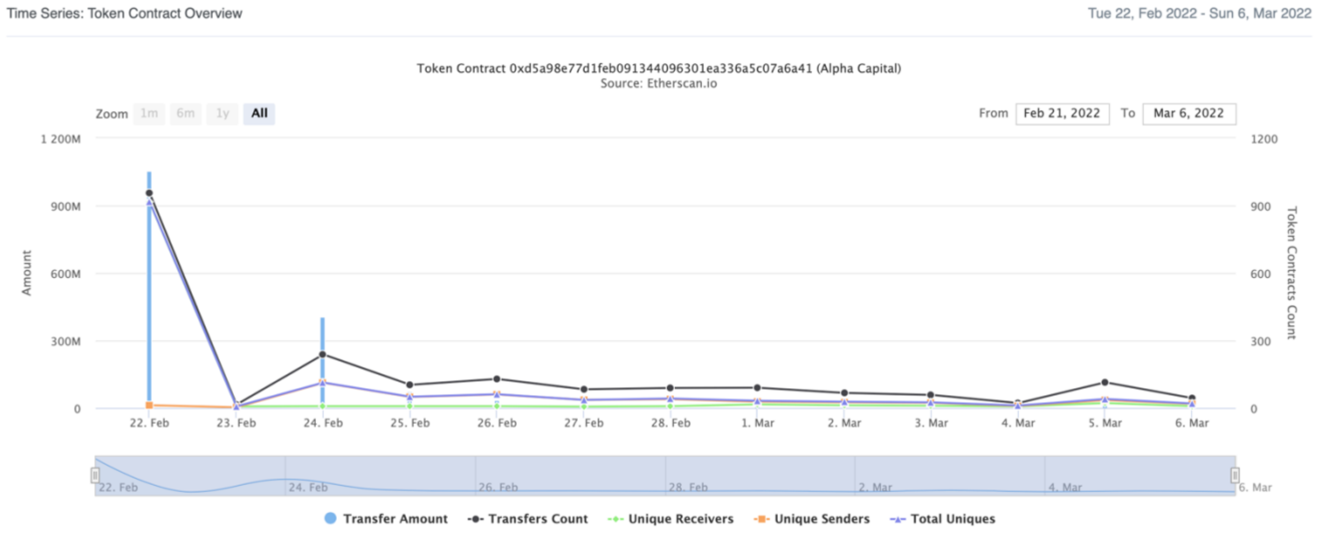
Alpha Capital Top 100 Token Holders

Source: Etherscan.io

OTHER ACCOUNTS
0x82a0a1477d2b68892128361410e19aeb2e1dd2b0
0x078b387757b1b65ef389abcb4c806556f910a019
0xc210b145611de349bfd57988f2ae66663d8d3b3d
0x96d3a216474ffa453db34bbeae7926e75b313d14
0x8d33320b0faebf1eb4c0f8ee6fa987c4a5dd30c3
0x6d1249c6706cf6bbd5fd18026f28c2ab4f147adb
0x0b09bbb590464cdeb953c0c81eb8c409cfe21e5b
0xf2061be4559b2356788c5c9eeb0773f31ba427b9 (Uniswap V2: ACAP 3)
0xcfabe48b39efdbe70e93c839eb973054b9be5b63
0xe940ea6d77bcc223a43bb41ace433cbfd39e3966

(A total of 948,759,364.12 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Alpha Capital Contract Interaction Details



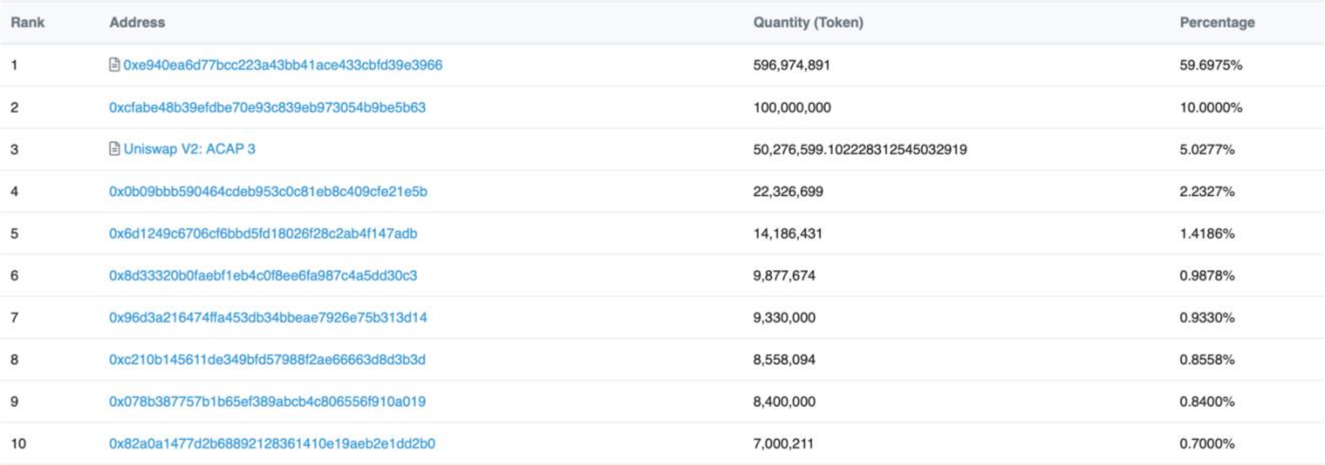
Time Series: Token Contract Overview

Tue 22, Feb 2022 - Sun 6, Mar 2022

Token Contract 0xd5a98e77d1feb091344096301ea336a5c07a6a41 (Alpha Capital)

Source: Etherscan.io

Alpha Capital Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	0xe940ea6d77bcc223a43bb41ace433cbfd39e3966	596,974,891	59.6975%
2	0xcfabe48b39efdbe70e93c839eb973054b9be5b63	100,000,000	10.0000%
3	Uniswap V2: ACAP 3	50,276,599.102228312545032919	5.0277%
4	0x0b09bbb590464cdeb953c0c81eb8c409cfe21e5b	22,326,699	2.2327%
5	0x6d1249c6706cf6bbd5fd18026f28c2ab4f147adb	14,186,431	1.4186%
6	0x8d33320b0faebf1eb4c0f8ee6fa987c4a5dd30c3	9,877,674	0.9878%
7	0x96d3a216474ffa453db34bbeae7926e75b313d14	9,330,000	0.9330%
8	0xc210b145611de349bfd57988f2ae66663d8d3b3d	8,558,094	0.8558%
9	0x078b387757b1b65ef389abcb4c806556f910a019	8,400,000	0.8400%
10	0x82a0a1477d2b68892128361410e19aeb2e1dd2b0	7,000,211	0.7000%

Contract functions details

+ [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #
  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens ($)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ [Int] IERC20Metadata (IERC20)
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IUniswapV2Pair
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf

```
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast
  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #

+ [Int] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+  Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
```

  - [Prv] _setOwner #

+ ERC20 (Context, IERC20, IERC20Metadata)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _beforeTokenTransfer #
  - [Int] _afterTokenTransfer #

+ [Lib] console
  - [Prv] _sendLogPayload
  - [Int] log
  - [Int] logInt
  - [Int] logUint
  - [Int] logString
  - [Int] logBool
  - [Int] logAddress
  - [Int] logBytes
  - [Int] logBytes1
  - [Int] logBytes2
  - [Int] logBytes3
  - [Int] logBytes4
  - [Int] logBytes5
  - [Int] logBytes6
  - [Int] logBytes7
  - [Int] logBytes8
  - [Int] logBytes9
  - [Int] logBytes10
  - [Int] logBytes11
  - [Int] logBytes12
  - [Int] logBytes13
  - [Int] logBytes14
  - [Int] logBytes15
  - [Int] logBytes16
  - [Int] logBytes17
  - [Int] logBytes18
  - [Int] logBytes19
  - [Int] logBytes20
  - [Int] logBytes21
  - [Int] logBytes22
  - [Int] logBytes23
  - [Int] logBytes24

- [Int] logBytes25
- [Int] logBytes26
- [Int] logBytes27
- [Int] logBytes28
- [Int] logBytes29
- [Int] logBytes30
- [Int] logBytes31
- [Int] logBytes32
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log

- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log

```
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
```

- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log

- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log

- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log
- [Int] log

```
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log
  - [Int] log

+ ACAP (ERC20, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC20,Ownable
  - [Ext] setBuybackWallet #
    - modifiers: onlyOwner
  - [Ext] setTreasuryWallet #
    - modifiers: onlyOwner
  - [Ext] setMarketingRate #
    - modifiers: onlyOwner
  - [Ext] setTreasuryRate #
    - modifiers: onlyOwner
  - [Ext] setReflectRate #
    - modifiers: onlyOwner
  - [Ext] setMinTokenBalance #
    - modifiers: onlyOwner
  - [Ext] rescueMarketingTokens #
    - modifiers: onlyOwner
  - [Ext] rescueTreasuryTokens #
    - modifiers: onlyOwner
  - [Ext] rescueReflectionTokens #
    - modifiers: onlyOwner
  - [Ext] addLiquidity ($)
    - modifiers: onlyOwner,liquidityAdd
  - [Ext] enableTrading #
    - modifiers: onlyOwner
  - [Ext] disableTrading #
    - modifiers: onlyOwner
  - [Ext] addReflection ($)
  - [Pub] isReflectionExcluded
  - [Ext] removeReflectionExcluded #
    - modifiers: onlyOwner
  - [Ext] addReflectionExcluded #
    - modifiers: onlyOwner
  - [Int] _addReflectionExcluded #
  - [Pub] isTaxExcluded
  - [Pub] addTaxExcluded #
```

  - modifiers: onlyOwner
- [Ext] removeTaxExcluded #
  - modifiers: onlyOwner
- [Pub] balanceOf
- [Int] _addBalance #
- [Int] _subtractBalance #
- [Int] _transfer #
- [Pub] unclaimedReflection
- [Int] _claimReflection #
- [Ext] claimReflection #
- [Int] _swap #
  - modifiers: lockSwap
- [Ext] swapAll #
- [Ext] withdrawAll #
  - modifiers: onlyOwner
- [Int] _takeTaxes #
- [Int] _getTaxAmounts
- [Int] _rawTransfer #
- [Ext] setMaxTransfer #
  - modifiers: onlyOwner
- [Ext] setSwapFees #
  - modifiers: onlyOwner
- [Pub] totalSupply
- [Int] _mint #
- [Ext] mint #
  - modifiers: onlyOwner
- [Ext] airdrop #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)

($) = payable function
# = non-constant function

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.	Low issues
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.	Passed
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. Out of gas

Issue:

- The function airdrop() uses the loop to make multiple minting to addresses. Fun ction will be aborted with OUT_OF_GAS exception if there will be a long addresses list.
- The function airdrop() do not check total minted amount to be lower than MAX_SUPPLY, that's may cause all function revert.

Recommendation:

Check that the array length is not too big and sum of the amounts is lower than MAX_SUPPLY.

Notes:

- Transfer function allows transfer if amount <= maxTxAmount or _inLiquidityAdd is true or _inSwap or owner is receiving.
- _reflectionExcluded logic is unused.

Owner privileges (In the period when the owner is not renounced)

- Owner can change buyback(marketing) and treasury wallets.
- Owner can change marketing, treasury and reflection rates.
- Owner can change minTokenBalance.
- Owner can withdraw totalMarketing, totalTreasury and totalReflected.
- Owner can mint tokens and add them to liquidity(total supply already minted).
- Owner can enable/disable trading.
- Owner can exclude/include in reflection (see notes).
- Owner can include/exclude from taxes.
- Owner can withdraw native tokens.
- Owner can change _maxTransfer amount.
- Owner can change swapFees.
- Owner can mint (total supply already minted).

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:
https://www.team.finance/view-coin/0xd5A98E77d1fEB091344096301Ea336a5C07a6A41?name=Alpha Capital&symbol=ACAP

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.