

TechRate
October, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

Gold Retriever (GLDN)



Deployer address

0xD2d7Ea9B838f1024577266CE3B24277828255348



Client contacts:

<https://twitter.com/0xGoldRetriever>



Blockchain

Ethereum



Project website:

<http://goldretriever.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 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 Gold Retriever (GLDN) to perform an audit of smart contracts:

<https://etherscan.io/token/0xfeeb4d0f5463b1b04351823c246bdb84c4320cc2#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 14.10.2022

Contract name Gold Retriever (GLDN)

Contract address 0xFeeB4D0f5463B1b04351823C246bdB84c4320CC2

Total supply 10,500,000

Token ticker GLDN

Decimals 18

Token holders 743

Transactions count 10,819

Top 100 holders dominance 91.99%

Amount rewards fee 28503457235892050713

**Sell Liquidity/ Marketing/
Rewards fees** 50 / 0 / 50

**Buy Liquidity/ Marketing/
Rewards fees** 0 / 0 / 100

pair 0x19A7C579e714e43c57997318FF0ba46A6D6891e4

Contract deployer address 0xD2d7Ea9B838f1024577266CE3B24277828255348

Owner address 0xD2d7Ea9B838f1024577266CE3B24277828255348

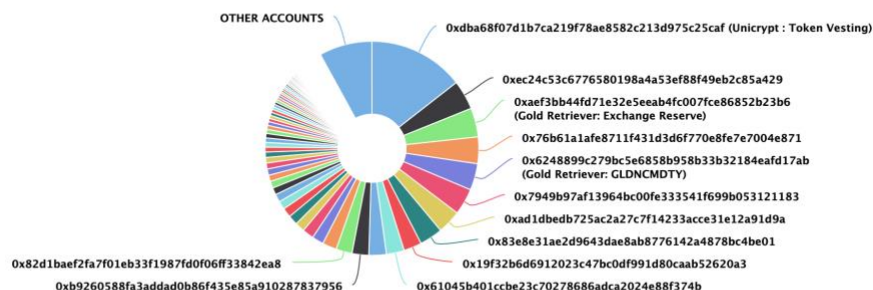
Gold Retriever (GLDN) Token Distribution

The top 100 holders collectively own 91.99% (9,658,962.22 Tokens) of Gold Retriever

Token Total Supply: 10,500,000.00 Token | Total Token Holders: 743

Gold Retriever Top 100 Token Holders

Source: Etherscan.io



(A total of 9,658,962.22 tokens held by the top 100 accounts from the total supply of 10,500,000.00 token)

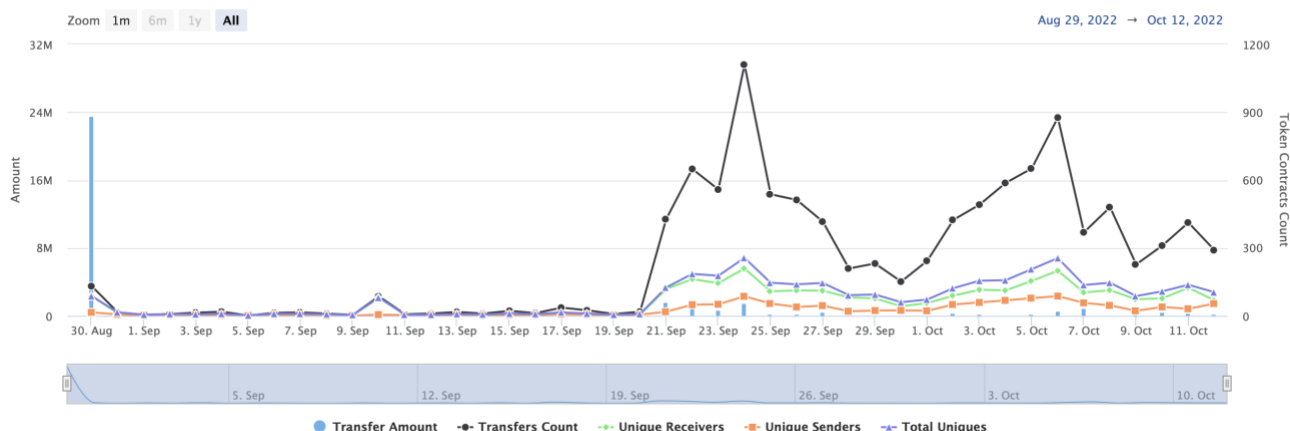
Gold Retriever (GLDN) Contract Interaction Details

Time Series: Token Contract Overview

Tue 30, Aug 2022 - Wed 12, Oct 2022

Token Contract 0xfeeb4d0f5463b1b04351823c246bdb84c4320cc2 (Gold Retriever)

Source: Etherscan.io



Gold Retriever (GLDN) Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Unicrypt : Token Vesting	1,520,763.884543429769621686	14.4835%
2	0xec24c53c6776580198a4a53ef88f49eb2c85a429	466,001	4.4381%
3	Gold Retriever: Exchange Reserve	460,178.424979834494674057	4.3827%
4	0x76b61a1afe8711f431d3d6f770e8fe7e7004e871	422,494.892054070390761884	4.0238%
5	Gold Retriever: GLDNCMDTY	420,712.331941757721299978	4.0068%
6	0x7949b97af13964bc00fe333541f699b053121183	419,930.005416008003389499	3.9993%
7	0xad1dbedb725ac2a27c7f1423acce31e12a91d9a	375,515.014867970106608056	3.5763%
8	0x83e8e31ae2d9643dae8ab8776142a4878bc4be01	367,827.94067029	3.5031%
9	0x19f32b6d6912023c47bc0df991d80caab52620a3	285,969.13500799177203971	2.7235%
10	0x61045b401ccbe23c70278686adca2024e88f374b	283,010.400018144369939963	2.6953%

Gold Retriever (GLDN) LP Token Holders

Rank	Address	Quantity	Percentage
1	Unicrypt : Liquidity Lockers	5,963.350416443638095891	97.3411%
2	0x04bda42de3bc32abb00df4600420442d4cf8287	108.68367577590669123	1.7741%
3	Gold Retriever: Deployer	35.669159803403942536	0.5822%
4	gldn97.eth	18.535763519441866104	0.3026%
5	Null Address: 0x000...000	0.000000000000001	0.0000%

Contract functions details

+ [Lib] SafeMathInt

- [Int] mul
- [Int] div
- [Int] sub
- [Int] add
- [Int] abs

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] allowance
- [Ext] transfer #
- [Ext] approve #
- [Ext] transferFrom #

+ [Int] IPancakeSwapPair

- [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] IPancakeSwapRouter

- [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
- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
- [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IPancakeSwapFactory

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

- + [Int] IDividendDistributor
 - [Ext] setDistributionCriteria #
 - [Ext] setShare #
 - [Ext] deposit (\$)
 - [Ext] process #
- + DividendDistributor (IDividendDistributor)
 - [Pub] <Constructor> #
 - [Ext] setDistributionCriteria #
 - modifiers: onlyToken
 - [Ext] setShare #
 - modifiers: onlyToken
 - [Ext] rescueToken #
 - modifiers: onlyToken
 - [Ext] deposit (\$)
 - modifiers: onlyToken
 - [Ext] process #
 - modifiers: onlyToken
 - [Int] shouldDistribute
 - [Int] distributeDividend #
 - [Ext] claimDividend #
 - [Pub] getUnpaidEarnings
 - [Int] getCumulativeDividends
 - [Int] addShareholder #
 - [Int] removeShareholder #
- + Ownable
 - [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] isOwner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Int] _transferOwnership #
- + ERC20Detailed (IERC20)
 - [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
- + GoldenRetrieverV2 (ERC20Detailed, Ownable)
 - [Pub] <Constructor> #
 - modifiers: ERC20Detailed,Ownable
 - [Ext] transfer #

- modifiers: validRecipient
- [Ext] transferFrom #
 - modifiers: validRecipient
- [Int] _basicTransfer #
- [Int] _transferFrom #
- [Int] takeFee #
- [Pub] manualSwap #
 - modifiers: onlyOwner,swapping
- [Int] addLiquidity #
 - modifiers: swapping
- [Int] swapBack #
 - modifiers: swapping
- [Prv] swapAndSendDivident #
- [Int] shouldTakeFee
- [Int] shouldAddLiquidity
- [Int] shouldSwapBack
- [Ext] setAutoAddLiquidity #
 - modifiers: onlyOwner
- [Ext] setAutoSwapBack #
 - modifiers: onlyOwner
- [Pub] enableClaimableExempt #
 - modifiers: onlyOwner
- [Ext] allowance
- [Ext] decreaseAllowance #
- [Ext] increaseAllowance #
- [Ext] approve #
- [Int] _approve #
- [Ext] checkFeeExempt
- [Pub] enableDisableTxLimit #
 - modifiers: onlyOwner
- [Pub] enableDisableWalletLimit #
 - modifiers: onlyOwner
- [Pub] setWhitelistTransfer #
 - modifiers: onlyOwner
- [Pub] setInitialDistribution #
 - modifiers: onlyOwner
- [Pub] setBuyFee #
 - modifiers: onlyOwner
- [Pub] setSellFee #
 - modifiers: onlyOwner
- [Ext] setIsDividendExempt #
 - modifiers: onlyOwner
- [Ext] setDistributionCriteria #
 - modifiers: onlyOwner
- [Ext] clearStuckBalance #

- modifiers: onlyOwner
- [Ext] rescueToken #
 - modifiers: onlyOwner
- [Ext] rescueDividentToken #
 - modifiers: onlyOwner
- [Pub] setFeeReceivers #
 - modifiers: onlyOwner
- [Ext] setDistributorSettings #
 - modifiers: onlyOwner
- [Pub] setMaxWalletLimit #
 - modifiers: onlyOwner
- [Pub] setMaxTxLimit #
 - modifiers: onlyOwner
- [Pub] getCirculatingSupply
- [Ext] isNotInSwap
- [Ext] manualSync #
- [Ext] setLP #
 - modifiers: onlyOwner
- [Pub] setAutomaticPairMarket #
 - modifiers: onlyOwner
- [Pub] getLiquidityBacking
- [Ext] setWhitelistFee #
 - modifiers: onlyOwner
- [Ext] setEdTxLimit #
 - modifiers: onlyOwner
- [Ext] setEdWalletLimit #
 - modifiers: onlyOwner
- [Ext] setBotBlacklist #
 - modifiers: onlyOwner
- [Ext] setMinSwapAmount #
 - modifiers: onlyOwner
- [Ext] totalSupply
- [Pub] balanceOf
- [Int] isContract
- [Prv] swapForMarketing #
- [Prv] swapForLiquidity #
- [Prv] addLiquidity #
- [Prv] swapTokensForEth #
- [Ext] <Fallback> (\$)
- [Pub] airDrop #
 - modifiers: onlyOwner

(\$) = 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.	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. Out of gas

Issue:

- The function `airDrop()` uses the loop to airdrop tokens from the list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:

Check that the array length is not too big.

2. No event on basic transfer

Issue:

- The function `_basicTransfer()` do not emit transferring event.

Recommendation:

Add event emitting.

Notes:

















- Old owner is not removed from exemptions after transferring ownership.

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



- Owner can call manual swap.
- Owner can enable/disable _autoAddLiquidity and _autoSwapBack.
- Owner can enable/disable ClaimableOnly.
- Owner can change EnableTransactionLimit, initialDistribution and checkWalletLimit status.
- Owner can whitelist addresses.
- Owner can change fees.
- Owner can exclude from dividends.
- Owner can change distribution criteria.
- Owner can withdraw ERC20 and ETH tokens.
- Owner can call distributors rescueToken function.
- Owner can change _marketingWalletAddress.
- Owner can change distributorGas.
- Owner can change MaxWalletLimit and MaxTxLimit.
- Owner can change pair address.
- Owner can include in automatedMarketMakerPairs array.
- Owner can exclude from limits.
- Owner can blacklist addresses.
- Owner can change swapTokensAtAmount.

Testnet deployment

Contracts Description Table

Contract	Type	Bases	Mutability	Modifiers
L	Function Name	Visibility		
GoldenRetrieverV2	Implementation	ERC20Detailed, Ownable		
L	transfer	External !		validRecipient
L	transferFrom	External !		validRecipient
L	setAutoAddLiquidity	External !		onlyOwner
L	setAutoSwapBack	External !		onlyOwner
L	enableClaimableExempt	Public !		onlyOwner
L	approve	External !		NO !
L	enableDisableTxLimit	Public !		onlyOwner
L	enableDisableWalletLimit	Public !		onlyOwner
L	setInitialDistribution	Public !		onlyOwner
L	setBuyFee	Public !		onlyOwner
L	setSellFee	Public !		onlyOwner
L	setIsDividendExempt	External !		onlyOwner
L	setMaxWalletLimit	Public !		onlyOwner
L	setMaxTxLimit	Public !		onlyOwner
L	setAutomaticPairMarket	Public !		onlyOwner
L	setMinSwapAmount	External !		onlyOwner

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details provided by the team:

<https://www.dextools.io/app/ether/pair-explorer/0x19a7c579e714e43c57997318ff0ba46a6d6891e4>

Tokens locking details provided by the team:

<https://app.unicrypt.network/amm/uni-v2/pair/0x19a7c579e714e43c57997318ff0ba46a6d6891e4>

Security score: 88.

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.