Cyberscope

Audit Report

GentleDogsCoin

August 2024

Network	BSC Testnet
Address	0x15b4d3c18f44297508911fb36b337f9886965400
Audited by	© cyberscope

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Contract Name	GentleDogsCoin
Testing Deploy	https://testnet.bscscan.com/address/0x90a5bbc643d5b2b8a32cc8f04288fff1ae6c77be
Symbol	GDCOIN
Decimals	18
Total Supply	1,789,000,000

Testing Deploy	https://testnet.bscscan.com/address/0x15b4d3c18f44297508911fb36b337f9886965400

Audit Updates

Initial Audit	18 Aug 2024

Source Files

Filename	SHA256
src/GentleDogsCoinGovernor.sol	ffd60c06edc2f506f87a5b45c6dadf01e31f24e8a8ede8796fa92a44a2c3b7fb
src/GentleDogsCoin.sol	fa53ab63e700f99e37f01952e5d454f84f5f79a2061010497887cac40dc139f1
src/interfaces/IEvents.sol	584ce440008c945c821b3726f168e6f4dec054d3ea9e5daf3db3455d4f8d1de5

src/interfaces/IErrors.sol	8ca8de41b786181d7eab32b9c48ba33e6 b29502a6bde9ce4f395de04bbf1478d

Overview

GentleDogsCoinGovernor.sol

The *GentleDogsCoinGovernor* contract is a custom governance smart contract built using OpenZeppelin's modular framework, designed to facilitate decentralized governance within the GentleDogsCoin ecosystem. It leverages several key OpenZeppelin extensions, including *GovernorVotes*, *GovernorVotesQuorumFraction*, and *GovernorCountingSimple*, to implement a voting system where token holders can propose and vote on decisions. The contract defines three immutable governance parameters—proposal threshold, voting delay, and voting period—ensuring consistent governance rules. A quorum of 4% of the total token supply is required for proposals to be valid, and the voting power is tied to the token holdings of participants. The contract's secure design is based on well-audited OpenZeppelin components, making it a robust solution for decentralized decision-making.

GentleDogsCoin.sol

The *GentleDogsCoin* contract is an ERC20 token implementation that incorporates various features such as staking, fee management, and governance. Built on OpenZeppelin's ERC20 extensions, the contract includes burnable and vote-enabled functionalities via *ERC20Burnable* and *ERC20Votes*, respectively, as well as off-chain signing through *ERC20Permit*. The contract allows token holders to stake their tokens in exchange for rewards, with different lock periods offering varying annual percentage yields (APY). The contract also includes governance controls, with an owner setting key parameters such as fees and the team wallet, and a designated governor managing fee adjustments. The contract ensures security and robustness through extensive checks, immutability of critical parameters, and careful handling of staking rewards and locking mechanisms. The initial token supply is minted to the contract owner.

Findings Breakdown

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	0	0	0	0

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
GentleDogsCoinGovernor	Implementation	Governor, GovernorVotes, GovernorVotesQuorumFraction, GovernorCountingSimple		
		Public	✓	Governor GovernorVotes GovernorVotesQuorumFraction
	votingDelay	Public		-
	votingPeriod	Public		-
	proposalThreshold	Public		-
GentleDogsCoin	Implementation	ERC20, ERC20Burnable, ERC20Votes, ERC20Permit, Ownable, IErrors, IEvents		
		Public	✓	ERC20 ERC20Permit Ownable
	setExcludedFromFee	External	✓	onlyOwner
	setTeamWallet	External	✓	onlyOwner
	setGovernor	External	✓	onlyOwner
	setFees	External	✓	onlyGovernor
	setAutomatedMarketMakerPair	Public	✓	onlyOwner

	addStakingRewards	External	✓	onlyOwner
	nonces	Public		-
	clock	Public		-
	CLOCK_MODE	Public		-
	deposit	External	✓	-
	withdraw	External	✓	-
	withdrawAll	External	✓	-
	emergencyWithdraw	External	✓	-
	claim	External	✓	-
	pendingRewards	Public		-
	_claim	Internal	✓	
	_withdraw	Internal	✓	
	_update	Internal	✓	
	_isBuy	Internal		
	_isSell	Internal		
	_getRate	Internal		

Inheritance Graph

See the detailed images in the github repository.

Flow Graph

See the detailed images in the github repository.

Summary

GentleDogsCoin contract implements a token, governance and staking mechanism. This audit investigates security issues, business logic concerns and potential improvements. GentleDogsCoin is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are 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.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

cyberscope.io