Cyberscope

Audit Report

GnomeMines Coin

October 2022

Type	BEP20
Network	BSC
Address	0x049CcA4B74D003575e28C840c8B956164f00f6e5
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	GnomeMinesCoin
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	100 runs
Explorer	https://bscscan.com/token/0x049CcA4B74D003575e28C840c8B956164f00f6e5
Symbol	GGCOIN
Decimals	18
Total Supply	10,000,000
Domain	https://gnomemines.com

Audit Updates

Initial Audit	14th October 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	75e3c97011e75627ffb36f4a2799a4e887e1a3e27ed427490e82d7b6f51cc5c9
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db8003d075c9c541019eb8dcf4122864d5
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
contracts/solidity/Token/AttributeMap.sol	2f19d2dedbdc8dbbd05052dbb80f409379658e34d70a93254362e5f5bb6516f2
contracts/solidity/Token/Authorized.sol	17663571ef5e99d927fd7ec7904c1f2c8087bd323387750c2a5066332244d1a5
contracts/solidity/Token/ERC20.sol	d6182e21dd249a443ce08bd9175175927c2fddf6afd1128c5342e8ea8ad1afe7
contracts/solidity/Token/GasHelper.sol	26422b9dc2a8f1d979970d1fec089c1abc802fa130588c302b6ec0fb5e8f7500
contracts/solidity/Token/GnomeMines.sol	84a473ffccb3f7a2ce499329bb73105382b5af26618be916054a4d47a457c9cd

contracts/solidity/Token/IPancake.sol	ba30eff0f25131078629051dd55ef67ff85d2a6b9747d2790f121b1a0930b313
contracts/solidity/Token/SwapHelper.sol	153351c0f6d07ff6199a36b1225daba58d93b111bc243208f4bbcfd58bae0a6a

Solidity Assembly MethodId Analysis

MethodId	Method Name
0x70a08231	balanceOf(address)
0x022c0d9f	swap(uint256, uint256, address, bytes)
0x23b872dd	transferFrom(address, address, uint256)
0xa9059cbb	transfer(address, uint256)
0x0dfe1681	token0( )
0x0902f1ac	getReserves( )

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Unresolved
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

ULTW - Transfers Liquidity to Team Wallet

Criticality	minor / informative
Location	contracts/solidity/Token/GnomeMines.sol#L168 contracts/solidity/Token/SwapHelper.sol#L13 contracts/solidity/Token/Authorized.sol#L13
Status	Unresolved

Description

The contract owner has the authority to transfer funds without limit to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the `buyBackAndHoldWithDecimals` and `safeWithdraw` method.

```
function buyBackAndHoldWithDecimals(uint decimalAmount, address receiver) public
isController {
    buyBackWithDecimals(decimalAmount, receiver);
  }

function safeWithdraw() external onlyOwner {
      payable(_msgSender()).transfer(address(this).balance);
 }

function safeWithdraw() external isAdmin {
payable(_msgSender()).transfer(address(this).balance); }
```

Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may volatile the token's price.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	TSDB	Total Supply Diversion from Balances	Unresolved
●	STC	Succeeded Transfer Check	Unresolved
●	FSA	Fixed Swap Address	Unresolved
●	CO	Code Optimization	Unresolved
●	MC	Missing Check	Unresolved
●	L01	Public Function could be Declared External	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved

TSDB - Total Supply Diversion from Balances

Criticality	medium
Location	contract.sol#L186
Status	Unresolved

Description

The contract has the ability to accumulate fees in the ‘accumulatedToAdmin’ variable. These fees are subtracted from the sender’s balance but not added to any balance. As a result, the sum of the balances might be diverse from the total supply. If the contract owner set variables like ‘_minAmountToAutoSwap’ to zero and ‘pausedSwapAdmin’ to false, then the ‘accumulatedToAdmin’ will never reset.

```
  function _transfer(
    address sender,
    address receiver,
    uint amount
  ) internal override {
    …
    …
    if (feeAmount != 0) splitFee(feeAmount, sender, adminFee);
    if ((!pausedSwapAdmin) && !isExemptSwapMaker(senderAttributes)) autoSwap(sender,
adminFee);
```

Recommendation

The contract should not allow the diversion between the total supply and the sum of the balances. The contract could temporarily transfer the fees to an address.

STC - Succeeded Transfer Check

Criticality	minor / informative
Location	contracts/solidity/Token/Authorized.sol#L12
Status	Unresolved

Description

According to the ERC20 specification, the transfer methods should be checked if the result is successful. Otherwise, the contract may wrongly assume that the transfer has been established.

```
 function safeTransfer(address token, address receiver, uint256 amount) external isAdmin { IERC20(token).transfer(receiver, amount); }
```

Recommendation

The contract should check if the result of the transfer methods is successful.

FSA - Fixed Swap Address

Criticality	minor / informative
Location	contracts/solidity/Token/GnomeMines.sol#L62
Status	Unresolved

Description

The swap address is assigned once in the constructor and it can not be changed. The decentralized swaps sometimes create a new swap version or abandon the current. A contract that cannot change the swap address may not be able to catch up with the upgrade.

```
constructor() ERC20(_nameToken, _symbolToken) {
    PancakeRouter router =
PancakeRouter(0x10ED43C718714eb63d5aA57B78B54704E256024E); // BSC
    liquidityPool = address(PancakeFactory(router.factory()).createPair(WBNB, address(this)));
```

Recommendation

It could be better to allow the swap address mutation in case of future swap updates.

CO - Code Optimization

Criticality	minor / informative
Location	contracts/solidity/Token/GnomeMines.sol#L280
Status	Unresolved

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes smaller, consumes less memory, executes more rapidly, or performs fewer operations.

The contract performs a redundant calculation. The `adminFee` and `totalFee` variables are the same.

```
function splitFee(
    uint incomingFeeTokenAmount,
    address sender,
    uint adminFee
  ) private {
    uint totalFee = adminFee;

    // Administrative distribution
    if (adminFee > 0) {
      accumulatedToAdmin += (incomingFeeTokenAmount * adminFee) / totalFee;
```

Recommendation

Rewrite some code segments so the runtime will be more performant.

MC - Missing Check

Criticality	minor / informative
Location	contracts/solidity/Token/GasHelper.sol#L10
Status	Unresolved

Description

The contract is processing variables that have not been properly sanitized and checked that they form the proper shape. These variables may produce vulnerability issues.

The variable swapFee can be set over the maximum swap fee percentage.

```
function setSwapFee(uint amount) external isAdmin { swapFee = amount; }
```

Recommendation

The contract should properly check the variables according to the required specifications.

It is recommended to embody a check to prevent the variable to be over 10000.

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contracts/solidity/Token/AttributeMap.sol#L12,18,43,19,48,46,14,45,49,13,15,50,16,17,47,44 contracts/solidity/Token/GnomeMines.sol#L153,100,163,168,158,136,108,172,96
Status	Unresolved

Description

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

```
isExemptFee
isSpecialFeeWalletReceiver
setExemptFee
setMaxTxAmount
isExemptSwapMaker
setSpecialFeeWallet
symbol
setExemptAmountLimit
isExemptTxLimit
...
```

Recommendation

Use the external attribute for functions never called from the contract.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contracts/solidity/Token/GnomeMines.sol#L20,16,28,34,29,23,17,24,19,27 contracts/solidity/Token/Authorized.sol#L9 contracts/solidity/Token/AttributeMap.sol#L9
Status	Unresolved

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
author
_nameToken
_maxAccountAmount
maxTotalFee
_minAmountToAutoSwap
decimal
_permissions
_attributeMap
_symbolToken
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contracts/solidity/Token/GnomeMines.sol#L142,163,158,153
Status	Unresolved

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
feeAdministrationWallet = administration
_minAmountToAutoSwap = amount
_maxAccountAmount = maxAccountAmount
_maxTxAmount = maxTxAmount
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
AttributeMap	Implementation	Authorized		
	isExemptFee	Public		-
	isExemptFeeReceiver	Public		-
	isExemptTxLimit	Public		-

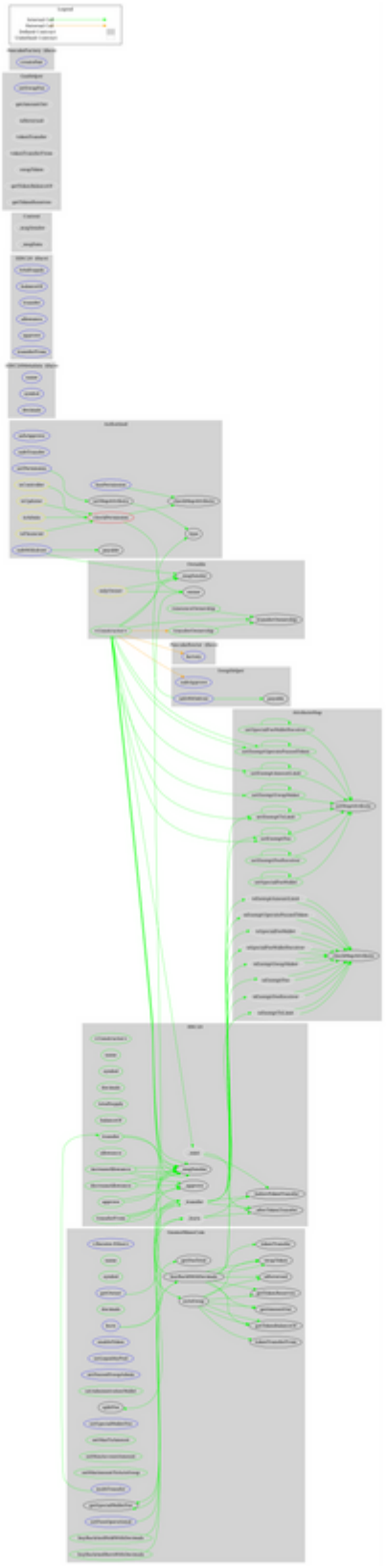
	isExemptAmountLimit	Public		-
	isExemptOperatePausedToken	Public		-
	isSpecialFeeWallet	Public		-
	isSpecialFeeWalletReceiver	Public		-
	isExemptSwapMaker	Public		-
	isExemptFee	Internal		
	isExemptFeeReceiver	Internal		
	isExemptTxLimit	Internal		
	isExemptAmountLimit	Internal		
	isExemptOperatePausedToken	Internal		
	isSpecialFeeWallet	Internal		
	isSpecialFeeWalletReceiver	Internal		
	isExemptSwapMaker	Internal		
	setExemptFee	Internal		
	setExemptFeeReceiver	Internal		
	setExemptTxLimit	Internal		
	setExemptAmountLimit	Internal		
	setExemptOperatePausedToken	Internal		
	setSpecialFeeWallet	Internal		
	setSpecialFeeWalletReceiver	Internal		
	setExemptSwapMaker	Internal		
	setExemptFee	Public	✓	isFinancial
	setExemptFeeReceiver	Public	✓	isFinancial
	setExemptTxLimit	Public	✓	isFinancial
	setExemptAmountLimit	Public	✓	isFinancial
	setExemptOperatePausedToken	Public	✓	isFinancial
	setSpecialFeeWallet	Public	✓	isFinancial
	setSpecialFeeWalletReceiver	Public	✓	isFinancial
	setExemptSwapMaker	Public	✓	isFinancial
Authorized	Implementation	Ownable		
	safeApprove	External	✓	isAdmin
	safeTransfer	External	✓	isAdmin
	safeWithdraw	External	✓	isAdmin
	setPermission	External	✓	isAdmin

	checkMapAttribute	Internal		
	setMapAttribute	Internal		
	hasPermission	External		-
	checkPermission	Private		
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
GasHelper	Implementation	AttributeMap		
	setSwapFee	External	✓	isAdmin
	getAmountOut	Internal		
	isReversed	Internal		
	tokenTransfer	Internal	✓	
	tokenTransferFrom	Internal	✓	
	swapToken	Internal	✓	

	getTokenBalanceOf	Internal		
	getTokenReserves	Internal		
GnomeMinesCoin	Implementation	GasHelper, ERC20		
	<Receive Ether>	External	Payable	-
	<Constructor>	Public	✓	ERC20
	name	Public		-
	symbol	Public		-
	getOwner	External		-
	decimals	Public		-
	getFeeTotal	Public		-
	getSpecialWalletFee	Public		-
	enableToken	External	✓	isAdmin
	setLiquidityPool	External	✓	isAdmin
	setPausedSwapAdmin	External	✓	isAdmin
	setAdministrationWallet	Public	✓	isAdmin
	setFeesOperational	External	✓	isFinancial
	setSpecialWalletFee	External	✓	isFinancial
	setMaxTxAmount	Public	✓	isFinancial
	setMaxAccountAmount	Public	✓	isFinancial
	setMinAmountToAutoSwap	Public	✓	isFinancial
	buyBackAndHoldWithDecimals	Public	✓	isController
	buyBackAndBurnWithDecimals	Public	✓	isController
	burn	External	✓	-
	multiTransfer	External	✓	-
	_transfer	Internal	✓	
	autoSwap	Private	✓	
	splitFee	Private	✓	
	buyBackWithDecimals	Private	✓	
PancakeFactory	Interface			
	createPair	External	✓	-

PancakeRouter	Interface			
	factory	External		-
SwapHelper	Implementation	Ownable		
	<Constructor>	Public	✓	-
	safeApprove	External	✓	onlyOwner
	safeWithdraw	External	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	gnomemines.com
Registry Domain ID	2662764423_DOMAIN_COM-VRSN
Creation Date	2021-12-19T18:36:09Z
Updated Date	2021-12-19T18:36:09Z
Registry Expiry Date	2023-12-19T18:36:09Z
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	https://www.godaddy.com
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain was created 10 months before the creation of the audit. It will expire in about 1 year.

There is no public billing information, the creator is protected by the privacy settings.

Summary

The Smart Contract analysis reported one minor severity issue. The contract owner has the authority to transfer funds to the team's wallet. Other than that, the contract owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a max limit of 10% fee.

Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

Cyberscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Cyberscope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Cyberscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The Cyberscope team disclaims any liability for the resulting losses.

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io