COINSCOPE

Audit Report

Henh

January 2022

Github https://github.com/prezano/HenHouse_Contracts

Audited by © coinscope

Table of Contents

Contract Review

The contract audit will review the files that are included in the github repository

Github	https://github.com/prezano/HenHouse_Contracts
Commit	96d49fcbef7aa672819809999f97b6c0fab7af6c
Files path	/contracts/Tokens

The audit review is based on the following files

File	**SHA256**
henHouse.sol	790badecb5cbc2733a3deb038527c84390dd3a70f501aa4aa2af8324e285e091
henHouseERC20.sol	2ffc1880dfbfe782a58a3602203b15c4ff84afeaa499359819cd34cbbe06d8bf
HenHouseRouter.sol	92dde86e5a8e80cd7d5200c100dc336f5db457f88421344b74ce469112638619

Audit Updates

Initial Audit	22th January 2022
Corrected	

Contract Analysis

🔴 Critical 🟠 Medium ⚪ Minor 🔵 Pass

Severity	Code	Description
🔵	ST	Contract Owner is not able to stop or pause transactions
🔵	OCTD	Contract Owner is not able to transfer tokens from specific address
🔵	OTUT	Owner Transfer User's Tokens
🔵	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
🔵	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
🟠	MT	Contract Owner is not able to mint new tokens
🔵	BT	Contract Owner is not able to burn tokens from specific wallet
🔵	BC	Contract Owner is not able to blacklist wallets from selling

MT - Mint Tokens

Criticality	medium
Location	henHouse.sol#L97

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `mintTokensOnHalvingSchedule` function in specific periods of time. As a result the contract tokens will be inflated.

We state that the owner privileges are necessary and required for proper business logic handling. Thus, we emphasise the users should be careful since the contract balance will be inflated.

```
function mintTokensOnHalvingSchedule() external onlyHalvingManager(_msgSender())
{...
```

Recommendation

The owner should carefully manage the credentials of the owner’s account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	CO	Code Optimization
●	L06	Missing Events Access Control
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions

CO - Code Optimization

Criticality	minor
Location	henHouse.sol#L49

Description

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

The antiBotTime variable is not initialized, thus the following expression will always yield false.

```
if (
    antiBotTime > block.timestamp &&
    amount > antiBotAmount &&
    bots[sender]
) {
    revert("Anti Bot");
}
```

Recommendation

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

L06 - Missing Events Access Control

Criticality	minor
Location	henHouse.sol#L49

Description

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

```
halvingManager = _hm
```

Recommendation

Emit an event for critical parameter changes.

L01 - Public Function could be Declared External

Criticality	minor
Location	HenHouseRouter.sol#L49,L205,L186 and 59 more

Description

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

```
setHalvingManager
decreaseAllowance
increaseAllowance
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	HenHouseRouter.sol#L22,L14,L40 and 12 more

Description

Constant state variables should be declared constant to save gas.

```
divPercent
maxSupply
antiBotTime
...
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	HenHouseRouter.sol#L73,L49,L89 and 35 more

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.

```
_bots
_hm
_type
...
```

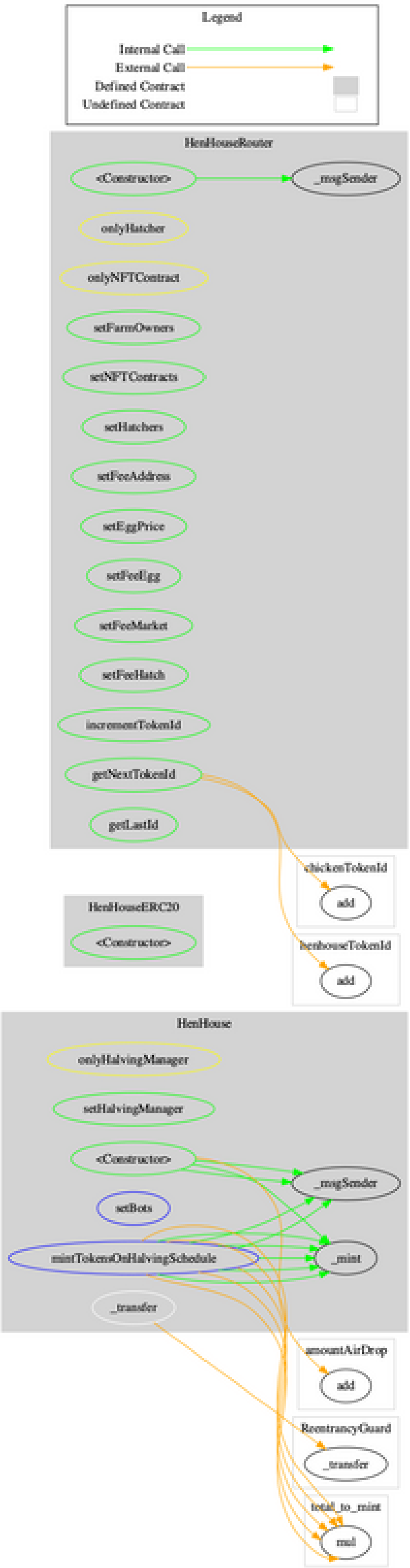
Recommendation

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

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
HenHouse	Implementation	HenHouseERC20, Reentrancy Guard		
	setHalvingManager	Public	✓	onlyOwner
	<Constructor>	Public	✓	HenHouseERC20
	setBots	External	✓	onlyOwner
	_transfer	Internal	✓	
	mintTokensOnHalvingSchedule	External	✓	onlyHalvingManager
HenHouseERC20	Implementation	Ownable, ERC20		
	<Constructor>	Public	✓	ERC20
HenHouseRouter	Implementation	Ownable		
	<Constructor>	Public	✓	-
	setFarmOwners	Public	✓	onlyOwner
	setNFTContracts	Public	✓	onlyOwner
	setHatchers	Public	✓	onlyOwner
	setFeeAddress	Public	✓	onlyOwner
	setEggPrice	Public	✓	onlyOwner
	setFeeEgg	Public	✓	onlyOwner
	setFeeMarket	Public	✓	onlyOwner
	setFeeHatch	Public	✓	onlyOwner
	incrementTokenId	Public	✓	onlyNFTContract
	getNextTokenId	Public		onlyNFTContract
	getLastId	Public		-

Contract Flow



Domain Info

Domain Name	henhouse.ar
Registry Domain ID	
Creation Date	2021-12-20T15:37:39+00:00
Updated Date	2022-01-06T10:14:02+00:00
Registry Expiry Date	2022-12-20T00:00:00+00:00
Registrar WHOIS Server	
Registrar URL	
Registrar	nicar
Registrar IANA ID	

The domain has been created about 1 month before the creation of the audit. It will expire in 11 months.

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

Summary

The contract analysis reported no compiler errors and only one medium threat issue. The contract owner has the authority to mint tokens. We state that the owner privileges are necessary and required for proper business logic handling. Thus, we emphasise the users should be careful since some predefined wallets will receive many tokens and the contract balance will be inflated. As a result the value of the rest holders will be decreased. There are no functions that can be abused by the owner to interrupt the user’s transactions.

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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

About Coinscope

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.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co