Audit Report

HellHound Token

December 2021

Type	FTM
Address	0x57E1B84Dc3Fee985Eb05A3e0648588aaFDB23E2C
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	Token
Compiler Version	v0.8.6+commit.11564f7e
Optimization	200 runs
Licence	MIT
Explorer	https://ftmscan.com/address/0x57e1b84dc3fee985eb05a3e0648588aafdb23e2c
Symbol	HELD
Decimals	18
Total Supply	100,000,000
Website	

Audit Updates

Initial Audit	11 December 2021
Corrected	

Contract Analysis

Pass	Description
✗	Contract Owner is not able to mint new tokens
✗	Contract Owner is not able to burn tokens from wallets
✓	Contract Owner is not able to increase fees more than a reasonable percent (up to 10%)
✓	Contract Owner is not able to pause or stop transactions
✓	Contract Owner is not able to transfer tokens from wallets
✓	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
✗	Contract Owner is not able to blacklist wallets from trading

MT - Mint Tokens

Criticality	high
Location	https://ftmscan.com/address/0x57e1b84dc3fee985eb05a3e0648588aafdb23e2c#code#L908

Description

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

```
    function mint(address _to, uint256 _amount)
        external
        onlyMinter
    {
        if (totalSupply() > MAX_SUPPLY) return;
        _mint(_to, _amount);
    }
```

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.

BT - Burn Tokens

Criticality	high
Location	https://ftmscan.com/address/0x57e1b84dc3fee985eb05a3e0648588aafdb23e2c#code#L916

Description

The contract owner has the authority to burn tokens from a specific address. The owner may take advantage of it by calling the `burn` function. As a result the targeted contract address will lose the corresponding tokens.

```
    function burn(address _from, uint256 _amount)
        external
        onlyMinter
    {
        _burn(_from, _amount);
    }
```

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.

BC - Blacklisted Contracts

Criticality	high
Location	https://ftmscan.com/address/0x57e1b84dc3fee985eb05a3e0648588aafdb23e2c#code

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `_setBot` function.

```
function _setBot(address from, bool value) external onlyOwner {
    _antibots[from] = value;
 }
```

Recommendation

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

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Initializable	Implementation			
	isConstructor	Private		
Context	Implementation	Initializable		
	__Context_init	Internal	✓	initializer
	__Context_init_unchained	Internal	✓	initializer
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Initializable, Context		
	__Ownable_init	Internal	✓	initializer
	__Ownable_init_unchained	Internal	✓	initializer
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner

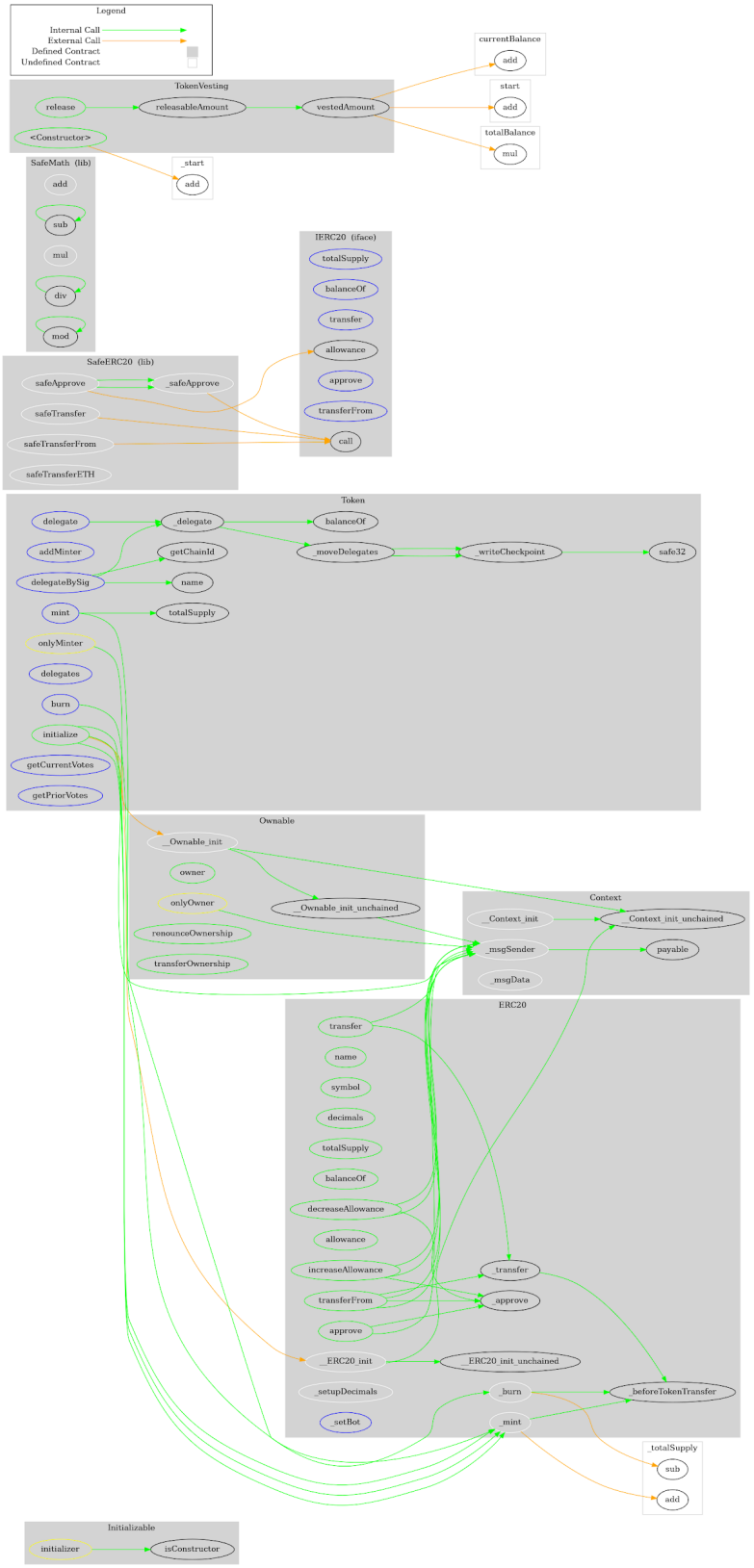
	transferOwnership	Public	✓	onlyOwner
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		

ERC20	Implementation	Initializable, Context, Ownable, IERC20		
	__ERC20_init	Internal	✓	initializer
	__ERC20_init_unchained	Internal	✓	initializer
	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	✓	
	_setupDecimals	Internal	✓	
	_setBot	External	✓	onlyOwner
	_beforeTokenTransfer	Internal		
SafeERC20	Library			
	_safeApprove	Internal	✓	
	safeApprove	Internal	✓	
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeTransferETH	Internal	✓	
TokenVesting	Implementation			
		Public	✓	-
	release	Public	✓	-
	releasableAmount	Public		-
	vestedAmount	Public		-
Token	Implementation	ERC20		

	initialize	Public	✓	initializer
	addMinter	External	✓	onlyOwner
	mint	External	✓	onlyMinter
	burn	External	✓	onlyMinter
	delegates	External		-
	delegate	External	✓	-
	delegateBySig	External	✓	-
	getCurrentVotes	External		-
	getPriorVotes	External		-
	_delegate	Internal	✓	
	_moveDelegates	Internal	✓	
	_writeCheckpoint	Internal	✓	
	safe32	Internal		
	getChainId	Internal		

Contract Flow



Summary

HellHound Token is an interesting project with a friendly and growing community. The contract analysis reported 3 critical issues. There are some functions that can be abused by the owner, like burning tokens from any wallet, minting new tokens to the owner and blacklisting addresses from being able to trade/sell again. A multi-wallet signing pattern or renouncing the ownership will eliminate all the contract threats. Finally, KYC or doxxing the team is advised in order to gain confidence and trust from the community.

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