Cyberscope

Audit Report

veHybrid

July 2022

SHA256 e986a8d54670a78826d50c1c515a88092896b83ee40dbc1b3fc8c1f0fc71a928

Audited by © cyberscope

Table of Contents

Contract Review

Contract Name	veHybrid
Test Deploy	https://testnet.bscscan.com/address/0xF20f2d2Cd9e5988b2C51fAB14DE03Be57CfF4A39#code
Symbol	veHFI
Decimals	18
Total Supply	-
Domain	https://hyfinance.net

Audit Updates

Initial Audit	15th July 2022
Corrected	20th July 2022

Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	754825f501dd014526eee0c415687b0f6c600533adfc872f7d45edb4f8b3b053
@openzeppelin/contracts/math/SafeMath.sol	f6d6214aa03f8dd6d6d14b7c15ffa387b3f1ce38ba3a215177baa132a44636e2
@openzeppelin/contracts/token/ERC20/ERC20.sol	22682313f68bee2d085fe1209047e9e55c0a076f7596d1058f29c265cef80a57
@openzeppelin/contracts/token/ERC20/IERC20.sol	c4b741712b8dc93ab3945205554a3ba2f80953e64d684e752d5a0fd07fc93f22
@openzeppelin/contracts/utils/Context.sol	eafb62c654640a07832b56e00902b4bf249633346585331af311c738b1c23bc5
contracts/veHybrid.sol	e986a8d54670a78826d50c1c515a88092896b83ee40dbc1b3fc8c1f0fc71a928

Contract Analysis

Critical Medium Minor Pass

Severity	Code	Description	Status
●	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	Multi-Sign
●	BT	Contract Owner is not able to burn tokens from specific wallet	Multi-Sign
●	BC	Contract Owner is not able to blacklist wallets from selling	

MT - Mint Tokens

Criticality	critical
Location	contract.sol#L25
Status	Multi-Sign

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 receiver, uint256 amount) external onlyMinter {
        require(receiver != address(0), "Recipient cannot be null");
        _mint(receiver, amount);
}
```

Recommendation

We state that the owner privileges are necessary and required for proper protocol operations. Thus, we emphasise the contract owner to be extra careful with the credentials. 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.

Updated 20 July 2022

The team has acknowledged that thread and transferred the contract ownership to a multi-sign mechanism.

BT - Burn Tokens

Criticality	critical
Location	contract.sol#L34
Status	Multi-Sign

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 burnFrom(address account, uint256 amount) external onlyMinter {
        _burn(account, amount);
}
```

Recommendation

We state that the owner privileges are necessary and required for proper protocol operations. Thus, we emphasise the contract owner to be extra careful with the credentials. 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.

Updated 20 July 2022

The team has acknowledged that thread and transferred the contract ownership to a multi-sign mechanism.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description	Status
	L04	Conformance to Solidity Naming Conventions	Acknowledged

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/veHybrid.sol#L20,8
Status	Acknowledged

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.

```
veHybrid
_minter
_status
```

Recommendation

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

Updated 20 July 2022

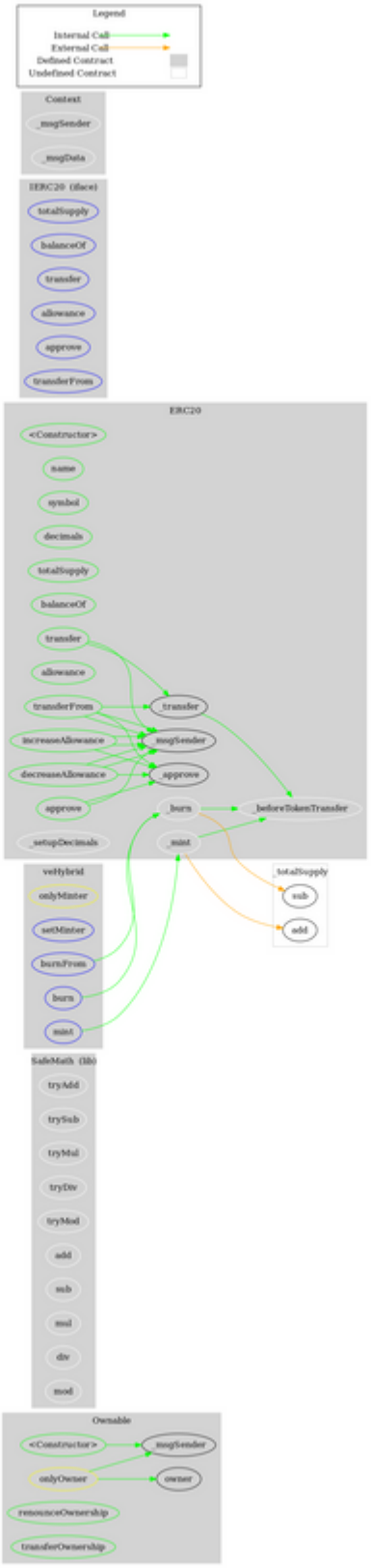
The team has acknowledged that it is not a security issue.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Ownable	Implementation	Context		
	<Constructor>	Internal	✓	
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
SafeMath	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		
ERC20	Implementation	Context, IERC20		
	<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	✓	
	_setupDecimals	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
veHybrid	Implementation	ERC20, Ownable		
	<Constructor>	Public	✓	ERC20
	setMinter	External	✓	onlyOwner
	mint	External	✓	onlyMinter
	burn	External	✓	-
	burnFrom	External	✓	onlyMinter
	_beforeTokenTransfer	Internal	✓	

Contract Flow



Domain Info

Domain Name	hyfinance.net
Registry Domain ID	2683607355_DOMAIN_NET-VRSN
Creation Date	2022-03-22T21:24:53.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	2023-03-22T21:24:53.00Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created in 8 months before the creation of the audit.

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

Summary

There are some functions that can be abused by the owner like minting tokens and burning tokens. if the contract owner abuses the mint functionality, then the contract will be highly inflated. The users could lost their tokens. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

Updated 20 July 2022

The team has transferred the contract ownership to a multi-sign mechanism.

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