Cyberscope

# Audit Report

# MigrateV2

July 2022

SHA256 88ab51a8ab28817f6f7ed01bd42c2972e61764069640a328f768b3175a71dbfb

Audited by © cyberscope

# Table of Contents

# Contract Review

| | |
|---|---|
| **Contract Name** | MigrateV2 |
| **Test Deploy** | https://testnet.bscscan.com/address/0x9795DcF2CfEe83456bCD4801eeB7a7f9c7A7551B |
| **Domain** | https://hyfinance.net |

# Audit Updates

| | |
|---|---|
| **Initial Audit** | 15th July 2022 |
| **Corrected** | |

# Source Files

| Filename | SHA256 |
| --- | --- |
| @openzeppelin/contracts/access/Ownable.sol | 754825f501dd014526eee0c415687b0f6c600533adfc872f7d45edb4f8b3b053 |
| @openzeppelin/contracts/math/SafeMath.sol | f6d6214aa03f8dd6d6d14b7c15ffa387b3f1ce38ba3a215177baa132a44636e2 |
| @openzeppelin/contracts/token/ERC20/IERC20.sol | c4b741712b8dc93ab3945205554a3ba2f80953e64d684e752d5a0fd07fc93f22 |
| @openzeppelin/contracts/token/ERC20/SafeERC20.sol | 74e10f4538df92e1c89140f16654914be8d7e9a66b24d6272ff0f28f89f8728b |
| @openzeppelin/contracts/utils/Address.sol | a22903d00a93aa211164d90ad11f01ccc7d34648114be89ec38c859fdea0f8d4 |
| @openzeppelin/contracts/utils/Context.sol | eafb62c654640a07832b56e00902b4bf249633346585331af311c738b1c23bc5 |
| @openzeppelin/contracts/utils/ReentrancyGuard.sol | a84a635e520d932183fc216c6f0ec109f8578149b15a91c728557a370430882a |
| contracts/interfaces/IERC20Meta.sol | 6d83cc8a7eb156aec4ac633bfe9d8bcc330654dddbecc6601f78bfafe9abb064 |
| contracts/interfaces/IHybrid.sol | aa66085ff86797073a673b3144a2377c6dba3d61ddb7a310e698ff8650afa2bb |
| contracts/MigrateV2.sol | 88ab51a8ab28817f6f7ed01bd42c2972e61764069640a328f768b3175a71dbfb |

# Introduction

Migration contract core functionality is to convert Hybrid Finance tokens to version 2 Hybrid Finance tokens. The convert ratio is defined by the circulating supply of the v1 token over the v2 balance of the MigrateV2 contract. As a result, the more converts are applied, the more balance will be decreased from the MigrateV2 contract. Hence, the rate formula will produce smaller numbers and the users will receive fewer v2 tokens. Essentially, the converter is not working as a strict bridge but more similar to a market maker mechanism.

# Contract Diagnostics

Critical Medium Minor

| 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 |
| | VCR | Variable Convert Ratio |
| | L04 | Conformance to Solidity Naming Conventions |
| | L07 | Missing Events Arithmetic |

# ST - Stop Transactions

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contract.sol#L52 |

## Description

The contract owner has the authority to stop transactions for all users. The owner may take advantage of it by setting the `deadline` to zero.

```
function convert() external nonReentrant {
        require(block.timestamp <= deadline, "Deadline passed");
```

## 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.

# OCTD - Owner Contract Tokens Drain

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contract.sol#L39 |

## Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the adminWithdraw function.

```
function adminWithdraw(address token, uint256 amount) external onlyOwner {
        require(IERC20Meta(token).balanceOf(address(this)) >= amount, "Amount too high");
        IERC20Meta(token).safeTransfer(msg.sender, amount);
}
```

## 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.

# VCR - Variable Convert Ratio

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contracts#L51 |

## Description

The migrator converts tokens proportionally to the balance of tokens that it holds. That means that it implements an exchange mechanism with variable rate, rather than a stable converter.

```
function convert() external nonReentrant {
        require(block.timestamp <= deadline, "Deadline passed");
        uint256 amount = hybrid.balanceOf(msg.sender);
        require(amount > 0, "Nothing to convert");
        uint256 rate = getRate();
        uint256 v2Amount = amount.mul(rate).div(1e18);
        hybrid.safeTransferFrom(msg.sender, DEAD, amount);
        hybridv2.safeTransfer(msg.sender, v2Amount);

        emit Converted(msg.sender, amount, v2Amount);
}
```

## Recommendation

The contract could keep the convert rate stable, otherwise it could be renamed to a definition closer to an exchange logic.

# L04 - Conformance to Solidity Naming Conventions

| | |
|---|---|
| **Criticality** | minor |
| **Location** | contracts/MigrateV2.sol#L34 |

## 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.

```
_deadline
```

## 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 |
| **Location** | contracts/MigrateV2.sol#L34 |

## 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.

```
deadline = _deadline
```

## Recommendation

Emit an event for critical parameter changes.

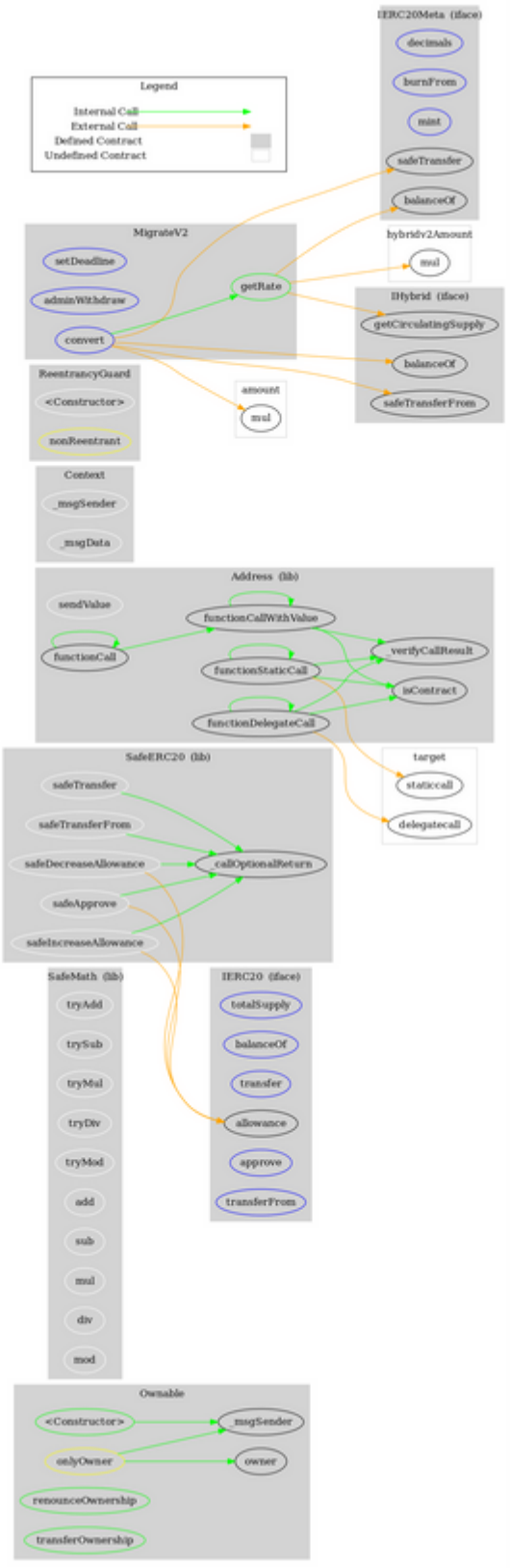
# Contract Functions

| 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 | | |
| | | | | |
| **IERC20** | Interface | | | |
| | totalSupply | External | | - |
| | balanceOf | External | | - |
| | transfer | External | ✓ | - |
| | allowance | External | | - |
| | approve | External | ✓ | - |
| | transferFrom | External | ✓ | - |
| | | | | |

| | | | | |
|---|---|---|---|---|
| **SafeERC20** | Library | | | |
| | safeTransfer | Internal | ✓ | |
| | safeTransferFrom | Internal | ✓ | |
| | safeApprove | Internal | ✓ | |
| | safeIncreaseAllowance | Internal | ✓ | |
| | safeDecreaseAllowance | Internal | ✓ | |
| | _callOptionalReturn | Private | ✓ | |
| | | | | |
| **Address** | Library | | | |
| | isContract | Internal | | |
| | sendValue | Internal | ✓ | |
| | functionCall | Internal | ✓ | |
| | functionCall | Internal | ✓ | |
| | functionCallWithValue | Internal | ✓ | |
| | functionCallWithValue | Internal | ✓ | |
| | functionStaticCall | Internal | | |
| | functionStaticCall | Internal | | |
| | functionDelegateCall | Internal | ✓ | |
| | functionDelegateCall | Internal | ✓ | |
| | _verifyCallResult | Private | | |
| | | | | |
| **Context** | Implementation | | | |
| | _msgSender | Internal | | |
| | _msgData | Internal | | |
| | | | | |
| **ReentrancyGuard** | Implementation | | | |
| | <Constructor> | Internal | ✓ | |
| | | | | |
| **IERC20Meta** | Interface | IERC20 | | |
| | decimals | External | | - |
| | burnFrom | External | ✓ | - |
| | mint | External | ✓ | - |
| | | | | |
| **IHybrid** | Interface | IERC20 | | |

| | | | | |
|---|---|---|---|---|
| | getCirculatingSupply | External | | - |
| | | | | |
| **MigrateV2** | Implementation | Ownable, ReentrancyGuard | | |
| | <Constructor> | Public | ✓ | - |
| | setDeadline | External | ✓ | onlyOwner |
| | adminWithdraw | External | ✓ | onlyOwner |
| | getRate | Public | | - |
| | convert | External | ✓ | nonReentrant |

# 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

MigrateV2 converts v1 for v2 tokens. There are some functions that can be abused by the owner like stopping transactions and transferring tokens to the team’s wallet. 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.

# 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