



Cyberscope

Audit Report

# Pulse Protocol

June 2022

SHA256 863b8a9b7ceaef9c80936bf210ed2bc3ce3b6142375e16aec7ff410d5c47f4a3

Audited by © cyberscope

# Table of Contents

|   |           |
|---|-----------|
| <b>Table of Contents</b>                                | <b>1</b>  |
| <b>Contract Review</b>                                  | <b>3</b>  |
| <b>Source Files</b>                                     | <b>3</b>  |
| <b>Audit Updates</b>                                    | <b>3</b>  |
| <b>Contract Analysis</b>                                | <b>4</b>  |
| <b>ULTW - Unlimited Liquidity to Team Wallet</b>        | <b>5</b>  |
| Description   | 5         |
| Recommendation  | 5         |
| <b>Contract Diagnostics</b>                             | <b>6</b>  |
| <b>MTS - Manipulate Total Supply</b>                    | <b>7</b>  |
| Description   | 7         |
| Recommendation  | 7         |
| <b>L01 - Public Function could be Declared External</b> | <b>8</b>  |
| Description   | 8         |
| Recommendation  | 8         |
| <b>L02 - State Variables could be Declared Constant</b> | <b>9</b>  |
| Description   | 9         |
| Recommendation  | 9         |
| <b>L04 - Conformance to Solidity Naming Conventions</b> | <b>10</b> |
| Description   | 10        |
| Recommendation  | 10        |
| <b>L07 - Missing Events Arithmetic</b>                  | <b>11</b> |
| Description   | 11        |
| Recommendation  | 11        |
| <b>L13 - Divide before Multiply Operation</b>           | <b>12</b> |
| Description   | 12        |

|                           |           |
|---------------------------|-----------|
| <b>Recommendation</b>     | <b>12</b> |
| <b>Contract Functions</b> | <b>13</b> |
| <b>Contract Flow</b>      | <b>18</b> |
| <b>Domain Info</b>        | <b>19</b> |
| <b>Summary</b>            | <b>20</b> |
| <b>Disclaimer</b>         | <b>21</b> |
| <b>About Cyberscope</b>   | <b>22</b> |

## Contract Review

|                         |   |
|-------------------------|---|
| <b>Contract Name</b>    | Pulse   |
| <b>Compiler Version</b> | v0.7.4+commit.3f05b770  |
| <b>Optimization</b>     | 200 runs  |
| <b>Testing Deploy</b>   | <a href="https://testnet.bscscan.com/token/0x44A2A45534e89A2528d21Ed757E3F51A64d6C4bf">https://testnet.bscscan.com/token/0x44A2A45534e89A2528d21Ed757E3F51A64d6C4bf</a> |
| <b>Domain</b>           | pulse-protocol.com  |

## Source Files

|                  |  |
|------------------|--|
| <b>Filename</b>  | <b>SHA256</b>  |
| <b>Pulse.sol</b> | 863b8a9b7ceaef9c80936bf210ed2bc3ce3b6142375e16aec7ff410d5c47f4a3 |

## Audit Updates

|                      |                |
|----------------------|----------------|
| <b>Initial Audit</b> | 11th June 2022 |
| <b>Corrected</b>     |                |

# 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  |

## ULTW - Unlimited Liquidity to Team Wallet

|             |                   |
|-------------|-------------------|
| Criticality | minor             |
| Location    | contract.sol#L904 |

### 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 `withdrawAllToTreasury()` method.

```
function withdrawAllToTreasury() external swapping onlyOwner {  
  
    uint256 amountToSwap = _gonBalances[address(this)].div(_gonsPerFragment);  
    require( amountToSwap > 0, "There is no Pulse token deposited in token  
contract");  
    address[] memory path = new address[](2);  
    path[0] = address(this);  
    path[1] = router.WETH();  
    router.swapExactTokensForETHSupportingFeeOnTransferTokens(  
        amountToSwap,  
        0,  
        path,  
        treasuryReceiver,  
        block.timestamp  
    );  
}
```

### 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

| Severity | Code | Description                                |
|----------|------|--|
| ●        | MTS  | Manipulate Total Supply                    |
| ●        | L01  | Public Function could be Declared External |
| ●        | L02  | State Variables could be Declared Constant |
| ●        | L04  | Conformance to Solidity Naming Conventions |
| ●        | L07  | Missing Events Arithmetic                  |
| ●        | L13  | Divide before Multiply Operation           |

## MTS - Manipulate Total Supply

|                    |                   |
|--------------------|-------------------|
| <b>Criticality</b> | minor             |
| <b>Location</b>    | contract.sol#L698 |

### Description

Owner is able to manipulate total supply. This change will have a direct impact on the token price and Market Cap.

```
for (uint256 i = 0; i < times; i++) {  
    _totalSupply = _totalSupply  
        .mul((10**RATE_DECIMALS).add(rebaseRate))  
        .div(10**RATE_DECIMALS);  
}
```

### Recommendation

The contract owner should carefully manage the adjustment of the circulating supply (increases or decreases), according to the token's price fluctuations.



## L01 - Public Function could be Declared External

|                    |  |
|--------------------|--|
| <b>Criticality</b> | minor  |
| <b>Location</b>    | contract.sol#L504,517,522,548,552,556,677,1074 |

### Description

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

```
getLiquidityBacking  
updatePancakeSwapRouter  
decimals  
symbol  
name  
transferOwnership  
renounceOwnership  
owner
```

### Recommendation

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

## L02 - State Variables could be Declared Constant

**Criticality**

minor

**Location**

contract.sol#L350,593,607,589

### Description

Constant state variables should be declared constant to save gas.

```
totalFee  
swapEnabled  
feeDenominator  
dividendsPerShareAccuracyFactor
```

### Recommendation

Add the constant attribute to state variables that never change.

## L04 - Conformance to Solidity Naming Conventions

|                    |   |
|--------------------|---|
| <b>Criticality</b> | minor   |
| <b>Location</b>    | contract.sol#L133,134,151,171,372,327,335,953,962,1025,1040,1065,1066,1067,1084,1088,1093,570,584,585,586,587,588,624,625,626,627,628,629 |

### 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.

```
_totalSupply  
_lastAddLiquidityTime  
_lastRebasedTime  
_initRebaseStartTime  
_autoAddLiquidity  
_autoRebase  
burnPitFee  
sellFee  
pulseDividendFee  
...
```

### 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**

contract.sol#L372

### 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.

```
minPeriod = _minPeriod
```

### Recommendation

Emit an event for critical parameter changes.

## L13 - Divide before Multiply Operation

**Criticality**

minor

**Location**

contract.sol#L443,681,1074

### Description

Performing divisions before multiplications may cause lose of prediction.

```
liquidityBalance = _gonBalances[pair].div(_gonsPerFragment)
times = deltaTime.div(900)
BUSD.transfer(addr_taxes, amount / 100 * 40)
BUSD.transfer(shareholder, amount / 100 * 60)
```

### Recommendation

The multiplications should be prior to the divisions.

# Contract Functions

| Contract                     | Type          | Bases      |            |           |
|------------------------------|---------------|------------|------------|-----------|
|                              | Function Name | Visibility | Mutability | Modifiers |
|                              |               |            |            |           |
| <b>SafeMathInt</b>           | Library       |            |            |           |
|                              | mul           | Internal   |            |           |
|                              | div           | Internal   |            |           |
|                              | sub           | Internal   |            |           |
|                              | add           | Internal   |            |           |
|                              |               |            |            |           |
| <b>SafeMath</b>              | Library       |            |            |           |
|                              | add           | Internal   |            |           |
|                              | sub           | Internal   |            |           |
|                              | sub           | Internal   |            |           |
|                              | mul           | Internal   |            |           |
|                              | div           | Internal   |            |           |
|                              | div           | Internal   |            |           |
|                              |               |            |            |           |
| <b>IERC20</b>                | Interface     |            |            |           |
|                              | totalSupply   | External   |            | -         |
|                              | balanceOf     | External   |            | -         |
|                              | allowance     | External   |            | -         |
|                              | transfer      | External   | ✓          | -         |
|                              | approve       | External   | ✓          | -         |
|                              | transferFrom  | External   | ✓          | -         |
|                              |               |            |            |           |
| <b>IPancakeSwap<br/>Pair</b> | Interface     |            |            |           |
|                              | name          | External   |            | -         |
|                              | symbol        | External   |            | -         |
|                              | decimals      | External   |            | -         |
|                              | totalSupply   | External   |            | -         |
|                              | balanceOf     | External   |            | -         |

|                            |                              |          |         |   |
|----------------------------|------------------------------|----------|---------|---|
|                            | allowance                    | External |         | - |
|                            | approve                      | External | ✓       | - |
|                            | transfer                     | External | ✓       | - |
|                            | transferFrom                 | External | ✓       | - |
|                            | DOMAIN_SEPARATOR             | External |         | - |
|                            | PERMIT_TYPEHASH              | External |         | - |
|                            | nonces                       | External |         | - |
|                            | permit                       | External | ✓       | - |
|                            | MINIMUM_LIQUIDITY            | External |         | - |
|                            | factory                      | External |         | - |
|                            | token0                       | External |         | - |
|                            | token1                       | External |         | - |
|                            | getReserves                  | External |         | - |
|                            | price0CumulativeLast         | External |         | - |
|                            | price1CumulativeLast         | External |         | - |
|                            | kLast                        | External |         | - |
|                            | mint                         | External | ✓       | - |
|                            | burn                         | External | ✓       | - |
|                            | swap                         | External | ✓       | - |
|                            | skim                         | External | ✓       | - |
|                            | sync                         | External | ✓       | - |
|                            | initialize                   | External | ✓       | - |
|                            |                              |          |         |   |
| <b>IPancakeSwap Router</b> | Interface                    |          |         |   |
|                            | factory                      | External |         | - |
|                            | WETH                         | External |         | - |
|                            | addLiquidity                 | External | ✓       | - |
|                            | addLiquidityETH              | External | Payable | - |
|                            | removeLiquidity              | External | ✓       | - |
|                            | removeLiquidityETH           | External | ✓       | - |
|                            | removeLiquidityWithPermit    | External | ✓       | - |
|                            | removeLiquidityETHWithPermit | External | ✓       | - |
|                            | swapExactTokensForTokens     | External | ✓       | - |
|                            | swapTokensForExactTokens     | External | ✓       | - |
|                            | swapExactETHForTokens        | External | Payable | - |

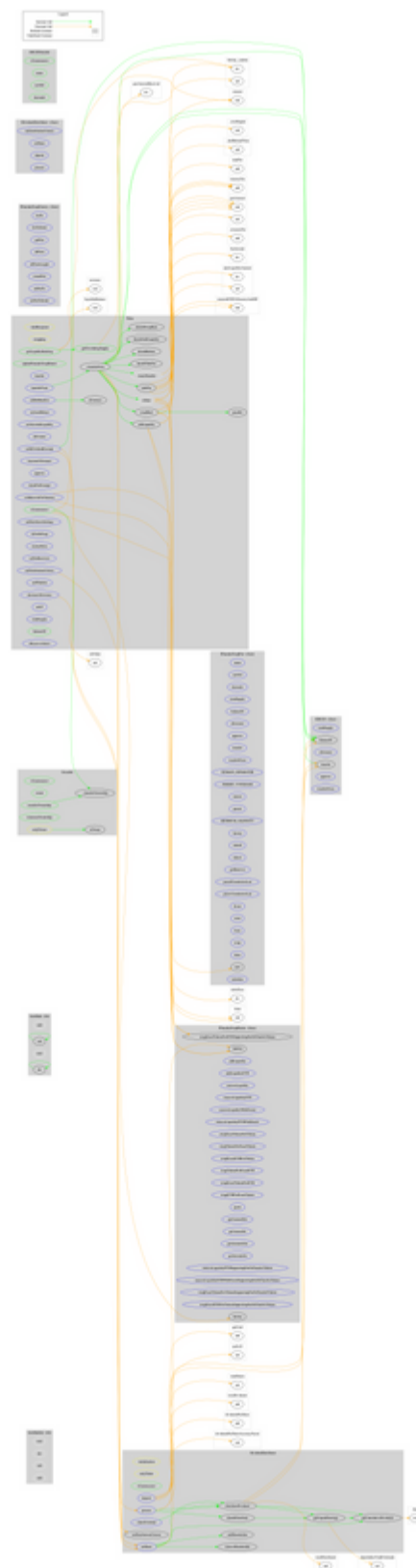
|                             |   |          |         |   |
|-----------------------------|---|----------|---------|---|
|                             | swapTokensForExactETH                                     | External | ✓       | - |
|                             | swapExactTokensForETH                                     | External | ✓       | - |
|                             | swapETHForExactTokens                                     | External | Payable | - |
|                             | quote   | External |         | - |
|                             | getAmountOut  | External |         | - |
|                             | getAmountIn   | External |         | - |
|                             | getAmountsOut   | External |         | - |
|                             | getAmountsIn  | External |         | - |
|                             | removeLiquidityETHSupportingFeeOnTransferTokens           | External | ✓       | - |
|                             | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External | ✓       | - |
|                             | swapExactTokensForTokensSupportingFeeOnTransferTokens     | External | ✓       | - |
|                             | swapExactETHForTokensSupportingFeeOnTransferTokens        | External | Payable | - |
|                             | swapExactTokensForETHSupportingFeeOnTransferTokens        | External | ✓       | - |
|                             |   |          |         |   |
| <b>IPancakeSwapFactory</b>  | Interface   |          |         |   |
|                             | feeTo   | External |         | - |
|                             | feeToSetter   | External |         | - |
|                             | getPair   | External |         | - |
|                             | allPairs  | External |         | - |
|                             | allPairsLength  | External |         | - |
|                             | createPair  | External | ✓       | - |
|                             | setFeeTo  | External | ✓       | - |
|                             | setFeeToSetter  | External | ✓       | - |
|                             |   |          |         |   |
| <b>IDividendDistributor</b> | Interface   |          |         |   |
|                             | setDistributionCriteria                                   | External | ✓       | - |
|                             | setShare  | External | ✓       | - |
|                             | deposit   | External | Payable | - |
|                             | process   | External | ✓       | - |
|                             |   |          |         |   |



| DividendDistributor  | Implementation          | IDividendDistributor      |         |                          |
|----------------------|-------------------------|---------------------------|---------|--------------------------|
|                      | <Constructor>           | Public                    | ✓       | -                        |
|                      | setDistributionCriteria | External                  | ✓       | onlyToken                |
|                      | setShare                | External                  | ✓       | onlyToken                |
|                      | deposit                 | External                  | Payable | onlyToken                |
|                      | process                 | External                  | ✓       | onlyToken                |
|                      | shouldDistribute        | Internal                  |         |                          |
|                      | distributeDividend      | Internal                  | ✓       |                          |
|                      | claimDividend           | External                  | ✓       | -                        |
|                      | getUnpaidEarnings       | Public                    |         | -                        |
|                      | getCumulativeDividends  | Internal                  |         |                          |
|                      | addShareholder          | Internal                  | ✓       |                          |
|                      | removeShareholder       | Internal                  | ✓       |                          |
|                      |                         |                           |         |                          |
| <b>Ownable</b>       | Implementation          |                           |         |                          |
|                      | <Constructor>           | Public                    | ✓       | -                        |
|                      | owner                   | Public                    |         | -                        |
|                      | isOwner                 | Public                    |         | -                        |
|                      | renounceOwnership       | Public                    | ✓       | onlyOwner                |
|                      | transferOwnership       | Public                    | ✓       | onlyOwner                |
|                      | _transferOwnership      | Internal                  | ✓       |                          |
|                      |                         |                           |         |                          |
| <b>ERC20Detailed</b> | Implementation          | IERC20                    |         |                          |
|                      | <Constructor>           | Public                    | ✓       | -                        |
|                      | name                    | Public                    |         | -                        |
|                      | symbol                  | Public                    |         | -                        |
|                      | decimals                | Public                    |         | -                        |
|                      |                         |                           |         |                          |
| <b>Pulse</b>         | Implementation          | ERC20Detailed,<br>Ownable |         |                          |
|                      | <Constructor>           | Public                    | ✓       | ERC20Detailed<br>Ownable |
|                      | updatePancakeSwapRouter | Public                    | ✓       | onlyOwner                |
|                      | rebase                  | Internal                  | ✓       |                          |
|                      | transfer                | External                  | ✓       | validRecipient           |

|  |                         |          |         |                       |
|--|-------------------------|----------|---------|-----------------------|
|  | transferFrom            | External | ✓       | validRecipient        |
|  | _basicTransfer          | Internal | ✓       |                       |
|  | _transferFrom           | Internal | ✓       |                       |
|  | takeFee                 | Internal | ✓       |                       |
|  | addLiquidity            | Internal | ✓       | swapping              |
|  | swapBack                | Internal | ✓       | swapping              |
|  | withdrawAllToTreasury   | External | ✓       | swapping<br>onlyOwner |
|  | shouldTakeFee           | Internal |         |                       |
|  | shouldRebase            | Internal |         |                       |
|  | shouldAddLiquidity      | Internal |         |                       |
|  | shouldSwapBack          | Internal |         |                       |
|  | setAutoRebase           | External | ✓       | onlyOwner             |
|  | setAutoAddLiquidity     | External | ✓       | onlyOwner             |
|  | allowance               | External |         | -                     |
|  | decreaseAllowance       | External | ✓       | -                     |
|  | increaseAllowance       | External | ✓       | -                     |
|  | approve                 | External | ✓       | -                     |
|  | checkFeeExempt          | External |         | -                     |
|  | setIsDividendExempt     | External | ✓       | onlyOwner             |
|  | setDistributionCriteria | External | ✓       | onlyOwner             |
|  | setDistributorSettings  | External | ✓       | onlyOwner             |
|  | getCirculatingSupply    | Public   |         | -                     |
|  | isNotInSwap             | External |         | -                     |
|  | manualSync              | External | ✓       | -                     |
|  | setFeeReceivers         | External | ✓       | onlyOwner             |
|  | getLiquidityBacking     | Public   |         | -                     |
|  | setWhitelist            | External | ✓       | onlyOwner             |
|  | setBotBlacklist         | External | ✓       | onlyOwner             |
|  | setLP                   | External | ✓       | onlyOwner             |
|  | totalSupply             | External |         | -                     |
|  | balanceOf               | Public   |         | -                     |
|  | isContract              | Internal |         |                       |
|  | <Receive Ether>         | External | Payable | -                     |

# Contract Flow



## Domain Info

|                               |   |
|-------------------------------|---|
| <b>Domain Name</b>            | pulse-protocol.com  |
| <b>Registry Domain ID</b>     | 1137702   |
| <b>Creation Date</b>          | 2022-05-22T00:00:00Z  |
| <b>Updated Date</b>           | 2022-05-22T00:00:00Z  |
| <b>Registry Expiry Date</b>   | 2023-05-22T00:00:00Z  |
| <b>Registrar WHOIS Server</b> | whois.ownregistrar.com  |
| <b>Registrar URL</b>          | <a href="http://www.ownregistrar.com">http://www.ownregistrar.com</a> |
| <b>Registrar</b>              | OwnRegistrar, Inc.  |
| <b>Registrar IANA ID</b>      | 1250  |

The domain has been created in 11 months before the creation of the audit.

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. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats. There is also a limit of max 25% fees.

## 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>