



# Smart Contract Audit

FOR

## Micropets2.0

DATED : 15 Aug 23'



# High Risk

## Centralization – Enabling Trades

**Severity:** High

**function:** enableTrading

**Status:** Open

### Overview:

The enableTrading function permits only the contract owner to activate trading capabilities. Until this function is executed, no investors can buy, sell, or transfer their tokens. This places a high degree of control and centralization in the hands of the contract owner.

```
function enableTrading() external onlyOwner {  
    require(!tradingActive, "Cannot enable trading again");  
    tradingActive = true;  
    swapEnabled = true;  
    tradingBlock = block.number;  
}
```

### Suggestion

To reduce centralization and potential manipulation, consider one of the following approaches:

1. Automatically enable trading after a specified condition, such as the completion of a presale, is met.
2. If manual activation is still desired, consider transferring the ownership of the contract to a trustworthy, third-party entity like a certified "PinkSale Safu" developer. This can provide investors with more confidence in the eventual activation of trading capabilities, mitigating concerns of potential bad faith actions by the original owner.



# High Risk

## Logical – Resetting fees

Severity: **High**

**function:** swapBack

**Status:** Open

### Overview:

**tokensForLiquidity** and **developmentAccrued** and **devAccrued** variables keep track of total accumulated fees. But these variables only reset to zero if **tokenForLiquidity > 0**

```
if (liquidityTokens > 0 && bnbForLiquidity > 0) {  
    addLiquidity(balanceOf(address(this)), bnbForLiquidity);  
    tokensForLiquidity = 0;  
    developmentAccrued = 0;  
    devAccrued = 0;  
}
```

### Suggestion

Ensure that all variables are reset to 0, regardless of whether **tokensForLiquidity** is bigger than 0 or not.

```
if (liquidityTokens > 0 && bnbForLiquidity > 0) {  
    addLiquidity(balanceOf(address(this)), bnbForLiquidity);  
}  
tokensForLiquidity = 0;  
developmentAccrued = 0;  
devAccrued = 0;
```



# AUDIT SUMMARY

**Project name - Micropets2.0**

**Date:** 15 Aug, 2023

**Scope of Audit-** Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

**Audit Status: Passed With High Risk**

## Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	2	0	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0



# USED TOOLS

---

## Tools:

### 1- Manual Review:

A line by line code review has been performed by audit ace team.

**2- BSC Test Network:** All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

### 3- Slither :

The code has undergone static analysis using Slither.

### Testnet version:

The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:

<https://testnet.bscscan.com/token/0xCA753A8260583e3140544C67fAbbD987aaF3F2EC>

---



# Token Information

---

**Token Name :** Micropets2.0

**Token Symbol:** Pets

**Decimals:** 18

**Token Supply:** 1,000,000,000

**Token Address:**

0x921072F8b876C9611E5aA1b744f03638d55833eB

**Checksum:**

2b43a640fff4c141a506c0df7504990321d0b3d6

**Owner:**

0xA928042e1ACE584372D0b96ADa872c259B6Fb7B

**(at time of writing the audit)**

**Deployer:**

0xA928042e1ACE584372D0b96ADa872c259B6Fb7B

---



# TOKEN OVERVIEW

---

**Fees:**

Buy Fees: 0-10%

Sell Fees: 0-10%

Transfer Fees: 0%

---

**Fees Privilege:** Owner

---

**Ownership:** not owned

---

**Minting:** No mint function

---

**Max Tx Amount/ Max Wallet Amount:** No

---

**Blacklist:** No

---

**Other Privileges:** Initial distribution of the tokens  
modifying fees  
enabling trades

---



# AUDIT METHODOLOGY

---

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
- Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

# VULNERABILITY CHECKLIST



Return values of low-level calls



**Gasless Send**



Private modifier



Using block.timestamp



Multiple Sends



Re-entrancy



Using Suicide



Tautology or contradiction



Gas Limit and Loops



Timestamp Dependence



Address hardcoded



Revert/require functions



Exception Disorder



Use of tx.origin



Using inline assembly



Integer overflow/underflow



Divide before multiply



Dangerous strict equalities



Missing Zero Address Validation



Using SHA3



Compiler version not fixed



Using throw



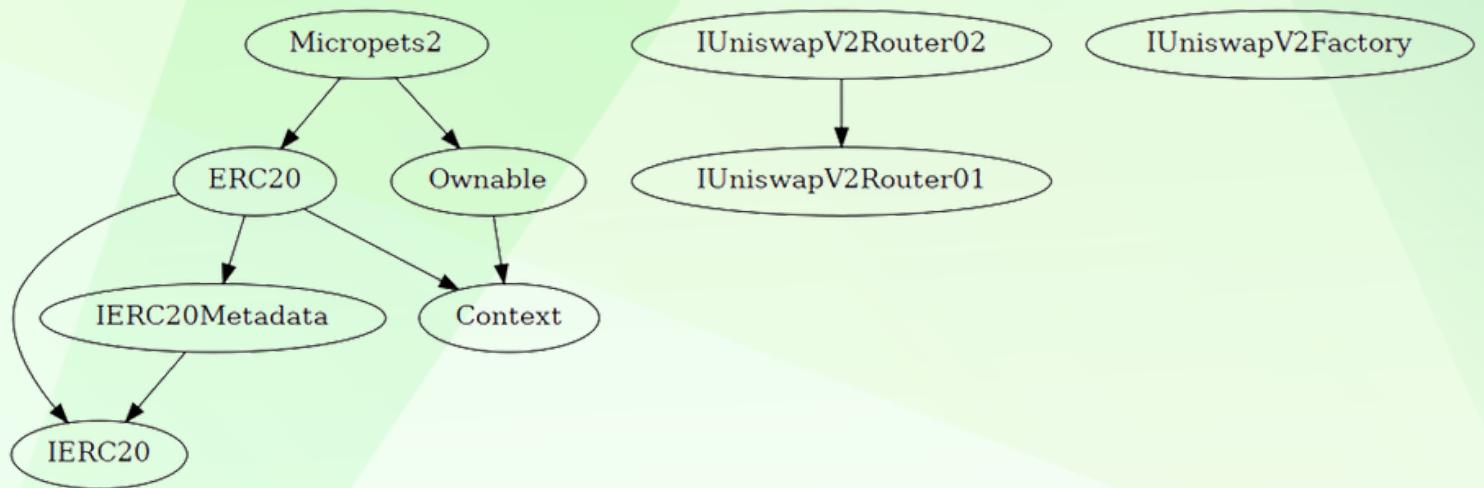
# CLASSIFICATION OF RISK

Severity	Description
◆ Critical	These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
◆ High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
◆ Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
◆ Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
◆ Gas Optimization / Suggestion	A vulnerability that has an informational character but is not affecting any of the code.

## Findings

Severity	Found
◆ Critical	0
◆ High-Risk	2
◆ Medium-Risk	0
◆ Low-Risk	0
◆ Gas Optimization / Suggestions	0

# INHERITANCE TREE





## POINTS TO NOTE

---

- **Owner is able to update buy/sell fees (0-10%)**
- Owner is not able to set fee on transfers
- Owner is not able to blacklist an arbitrary address.
- Owner is not able to disable trades
- Owner is not able to mint new tokens
- Owner is not able to set maximum wallet and maximum buy/sell limits



# CONTRACT ASSESSMENT

Contract	Type	Bases			
:					
└  **Function Name**   **Visibility**   **Mutability**   **Modifiers**					
**IERC20**   Interface					
└  totalSupply   External !    NO !					
└  balanceOf   External !    NO !					
└  transfer   External !   ●  NO !					
└  allowance   External !    NO !					
└  approve   External !   ●  NO !					
└  transferFrom   External !   ●  NO !					
**IERC20Metadata**   Interface   IERC20					
└  name   External !    NO !					
└  symbol   External !    NO !					
└  decimals   External !    NO !					
**Context**   Implementation					
└  _msgSender   Internal 🔒					
└  _msgData   Internal 🔒					
**ERC20**   Implementation   Context, IERC20, IERC20Metadata					
└  <Constructor>   Public !   ●  NO !					
└  name   Public !    NO !					
└  symbol   Public !    NO !					
└  decimals   Public !    NO !					
└  totalSupply   Public !    NO !					
└  balanceOf   Public !    NO !					
└  transfer   Public !   ●  NO !					
└  allowance   Public !    NO !					
└  approve   Public !   ●  NO !					
└  transferFrom   Public !   ●  NO !					
└  increaseAllowance   Public !   ●  NO !					
└  decreaseAllowance   Public !   ●  NO !					
└  _transfer   Internal 🔒   ●					
└  _mint   Internal 🔒   ●					
└  _burn   Internal 🔒   ●					
└  _approve   Internal 🔒   ●					
└  _spendAllowance   Internal 🔒   ●					



# CONTRACT ASSESSMENT

```
| ⊢ | _beforeTokenTransfer | Internal 🔒 | ● |||
| ⊢ | _afterTokenTransfer | Internal 🔒 | ● |||
|||||
| **Ownable** | Implementation | Context ||
| ⊢ | <Constructor> | Public ! | ●|NO ! |
| ⊢ | owner | Public ! | |NO ! |
| ⊢ | _checkOwner | Internal 🔒 | |||
| ⊢ | renounceOwnership | Public ! | ●| onlyOwner |
| ⊢ | transferOwnership | Public ! | ●| onlyOwner |
| ⊢ | _transferOwnership | Internal 🔒 | ● |||
|||||
| **IUniswapV2Router01** | Interface |||
| ⊢ | factory | External ! | |NO ! |
| ⊢ | WETH | External ! | |NO ! |
| ⊢ | addLiquidity | External ! | ●|NO ! |
| ⊢ | addLiquidityETH | External ! | 💸|NO ! |
| ⊢ | removeLiquidity | External ! | ●|NO ! |
| ⊢ | removeLiquidityETH | External ! | ●|NO ! |
| ⊢ | removeLiquidityWithPermit | External ! | ●|NO ! |
| ⊢ | removeLiquidityETHWithPermit | External ! | ●|NO ! |
| ⊢ | swapExactTokensForTokens | External ! | ●|NO ! |
| ⊢ | swapTokensForExactTokens | External ! | ●|NO ! |
| ⊢ | swapExactETHForTokens | External ! | 💸|NO ! |
| ⊢ | swapTokensForExactETH | External ! | ●|NO ! |
| ⊢ | swapExactTokensForETH | External ! | ●|NO ! |
| ⊢ | swapETHForExactTokens | External ! | 💸|NO ! |
| ⊢ | quote | External ! | |NO ! |
| ⊢ | getAmountOut | External ! | |NO ! |
| ⊢ | getAmountIn | External ! | |NO ! |
| ⊢ | getAmountsOut | External ! | |NO ! |
| ⊢ | getAmountsIn | External ! | |NO ! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 ||
| ⊢ | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ●|NO ! |
| ⊢ | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ●|NO ! |
| ⊢ | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ●|NO ! |
| ⊢ | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | 💸|NO ! |
| ⊢ | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ●|NO ! |
|||||
```



# CONTRACT ASSESSMENT

```
| **|UniswapV2Factory** | Interface | |||
| ⊂ | feeTo | External ! | NO ! |
| ⊂ | feeToSetter | External ! | NO ! |
| ⊂ | getPair | External ! | NO ! |
| ⊂ | allPairs | External ! | NO ! |
| ⊂ | allPairsLength | External ! | NO ! |
| ⊂ | createPair | External ! | ● | NO ! |
| ⊂ | setFeeTo | External ! | ● | NO ! |
| ⊂ | setFeeToSetter | External ! | ● | NO ! |
|||||
| **Micropets2** | Implementation | ERC20, Ownable ||
| ⊂ | <Constructor> | Public ! | ● | ERC20 |
| ⊂ | airdropToWallets | External ! | ● | onlyOwner |
| ⊂ | <Receive Ether> | External ! | ● | NO ! |
| ⊂ | enableTrading | External ! | ● | onlyOwner |
| ⊂ | _transfer | Internal 🔒 | ● |
| ⊂ | swapBack | Private 🔒 | ● |
| ⊂ | swapTokensForBNB | Internal 🔒 | ● |
| ⊂ | safeTransferBNB | Internal 🔒 | ● |
| ⊂ | addLiquidity | Private 🔒 | ● |
| ⊂ | excludeFromFees | Public ! | ● | onlyOwner |
| ⊂ | _setAutomatedMarketMakerPair | Private 🔒 | ● |
| ⊂ | setAutomatedMarketMakerPair | External ! | ● | onlyOwner |
| ⊂ | updateBuyFees | External ! | ● | onlyOwner |
| ⊂ | updateSellFees | External ! | ● | onlyOwner |
| ⊂ | updateDevelopmentWallet | External ! | ● | onlyOwner |
| ⊂ | updateTeamWallet | External ! | ● | onlyOwner |
| ⊂ | updateLiquidityWallet | External ! | ● | onlyOwner |
| ⊂ | updateSwapTokensAtAmount | External ! | ● | onlyOwner |
| ⊂ | claimStuckTokens | External ! | ● | onlyOwner |
```

## ### Legend

Symbol	Meaning
-----	-----
●	Function can modify state
💵	Function is payable



# STATIC ANALYSIS

```
INFO:Detectors:
Different versions of Solidity are used:
- Version used: ['>=0.5.0', '>=0.6.2', '^0.8.0', '^0.8.17']
- >=0.5.0 (contracts/Token.sol#853)
- >=0.6.2 (contracts/Token.sol#649)
- >=0.6.2 (contracts/Token.sol#802)
- ^0.8.0 (contracts/Token.sol#98)
- ^0.8.0 (contracts/Token.sol#125)
- ^0.8.0 (contracts/Token.sol#150)
- ^0.8.0 (contracts/Token.sol#562)
- ^0.8.17 (contracts/Token.sol#8)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
Context._msgData() (contracts/Token.sol#142-144) is never used and should be removed
ERC20._burn(address,uint256) (contracts/Token.sol#450-466) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.8.17 (contracts/Token.sol#8) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#98) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#125) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#150) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#562) allows old versions
Pragma version>=0.6.2 (contracts/Token.sol#649) allows old versions
Pragma version>=0.6.2 (contracts/Token.sol#802) allows old versions
Pragma version>=0.5.0 (contracts/Token.sol#853) allows old versions
solc-0.8.17 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Micropets2.safeTransferBNB(address,uint256) (contracts/Token.sol#1119-1122):
- (success) = to.call(value: value)(new bytes(0)) (contracts/Token.sol#1120)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IUniswapV2Router01.WETH() (contracts/Token.sol#654) is not in mixedCase
Event Micropets2.developmentWalletUpdated(address,address) (contracts/Token.sol#919-922) is not in CapWords
Parameter Micropets2.updateBuyFees(uint256,uint256,uint256)._developmentFee (contracts/Token.sol#1162) is not in mixedCase
Parameter Micropets2.updateBuyFees(uint256,uint256,uint256)._liquidityFee (contracts/Token.sol#1163) is not in mixedCase
Parameter Micropets2.updateBuyFees(uint256,uint256,uint256)._teamFee (contracts/Token.sol#1164) is not in mixedCase
Parameter Micropets2.updateSellFees(uint256,uint256)._developmentFee (contracts/Token.sol#1174) is not in mixedCase
Parameter Micropets2.updateSellFees(uint256,uint256)._liquidityFee (contracts/Token.sol#1175) is not in mixedCase
Parameter Micropets2.claimStuckTokens(address)._token (contracts/Token.sol#1216) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#659) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#660)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
Micropets2.constructor(uint256) (contracts/Token.sol#932-964) uses literals with too many digits:
- swapTokensAtAmount = (initialSupply * 1) / 100000 (contracts/Token.sol#954)
Micropets2.updateSwapTokensAtAmount(uint256) (contracts/Token.sol#1201-1214) uses literals with too many digits:
- require(bool,string)(newAmount >= (totalsupply() * 1) / 100000,Swap amount cannot be lower than 0.001% total supply.) (contracts/Token.sol#1204-1207)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Slither:./contracts/Token.sol analyzed (9 contracts with 88 detectors), 41 result(s) found
```

**Result => A static analysis of contract's source code has been performed using slither,  
No major issues were found in the output**



# FUNCTIONAL TESTING

## 1- Adding liquidity (**passed**):

<https://testnet.bscscan.com/tx/0xdfa9533ea8e6ac3fc5651fef36e21945145b72b1bbb5f46f1cbc5b5bf62ef19d>

## 2- Buying when excluded (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x653491514a50ba41f5a8186190df2c277a4392d0b70e437314b00fc3aec47f9>

## 3- Selling when excluded (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x086ada39a0cd4f1a75fe67aa73462840736982e200b97baf827d4c22c83c019d>

## 4- Transferring when excluded from fees (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x6814257d7ae741d78355c59948ee1b0a547e4c66af6d06738cbff9225912e86e>

## 5- Buying when not excluded from fees (tax adjustable in range 0-10%) (**passed**):

<https://testnet.bscscan.com/tx/0xbe842ff6e279ba89be90ea51388dc707f8723c407de874eaae8eac6ab4dc7ab6>

## 6- Selling when not excluded from fees (tax adjustable in range 0-10%) (**passed**):

<https://testnet.bscscan.com/tx/0xa4fb7675acdfb6d4adf21f014766aeb121ba556acb871dfdd89eb38ebaac920a>



# FUNCTIONAL TESTING

---

**7- Transferring when not excluded from fees (0% tax ) (passed):**

<https://testnet.bscscan.com/tx/0x5a680b0629c3b6d372b2508053f029b267a10a5236664a123095155fe0926d52>

**8- Internal swap (0% tax ) (passed):**

<https://testnet.bscscan.com/tx/0x5a680b0629c3b6d372b2508053f029b267a10a5236664a123095155fe0926d52>



# High Risk

## Centralization – Enabling Trades

**Severity:** High

**function:** enableTrading

**Status:** Open

### Overview:

The enableTrading function permits only the contract owner to activate trading capabilities. Until this function is executed, no investors can buy, sell, or transfer their tokens. This places a high degree of control and centralization in the hands of the contract owner.

```
function enableTrading() external onlyOwner {  
    require(!tradingActive, "Cannot enable trading again");  
    tradingActive = true;  
    swapEnabled = true;  
    tradingBlock = block.number;  
}
```

### Suggestion

To reduce centralization and potential manipulation, consider one of the following approaches:

1. Automatically enable trading after a specified condition, such as the completion of a presale, is met.
2. If manual activation is still desired, consider transferring the ownership of the contract to a trustworthy, third-party entity like a certified "PinkSale Safu" developer. This can provide investors with more confidence in the eventual activation of trading capabilities, mitigating concerns of potential bad faith actions by the original owner.



# High Risk

## Logical – Resetting fees

Severity: **High**

**function:** swapBack

**Status:** Open

### Overview:

**tokensForLiquidity** and **developmentAccrued** and **devAccrued** variables keep track of total accumulated fees. But these variables only reset to zero if **tokenForLiquidity > 0**

```
if (liquidityTokens > 0 && bnbForLiquidity > 0) {  
    addLiquidity(balanceOf(address(this)), bnbForLiquidity);  
    tokensForLiquidity = 0;  
    developmentAccrued = 0;  
    devAccrued = 0;  
}
```

### Suggestion

Ensure that all variables are reset to 0, regardless of whether **tokensForLiquidity** is bigger than 0 or not.

```
if (liquidityTokens > 0 && bnbForLiquidity > 0) {  
    addLiquidity(balanceOf(address(this)), bnbForLiquidity);  
}  
tokensForLiquidity = 0;  
developmentAccrued = 0;  
devAccrued = 0;
```



# 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. 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 Auditace 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 Auditace 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 Auditace team disclaims any liability for the resulting losses.



# ABOUT AUDITACE

---

We specialize in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.



**<https://auditace.tech/>**



**[https://t.me/Audit\\_Ace](https://t.me/Audit_Ace)**



**[https://twitter.com/auditace\\_](https://twitter.com/auditace_)**



**<https://github.com/Audit-Ace>**

---