



APE SALE

Smart Contract Security Audit



Project: WorkOut

Website: <https://workoutnft.io>



Low-Risk

1 low-risk code
issue found



Medium-Risk

1 medium-risk code
issue found



High-Risk

0 high-risk code issue
found

Contract Address

0xd249b7955ec439592b77453b8fed7f7b0c1f1dd5

Disclaimer: ApeSale is not responsible for any financial losses. Nothing in this contract audit is a financial advice, please do your own research.

Disclaimer

ApeSale is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

ApeSale is not responsible for any financial losses. Nothing in this contract audit is a financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. ApeSale does not endorse, recommend, support or suggest to invest in any project.

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0xd249b7955ec439592b77453b8fed7f7b0c1f1dd5	1,000,000,000	100% for Presale & Liquidity

Source Code

ApeSale was commissioned by WorkOut to perform an audit based on the following smart contract:

<https://bscscan.com/address/0xd249b7955ec439592b77453b8fed7f7b0c1f1dd5#code>

● **Medium-Risk:** Could be fixed, will not bring problems.

Contract can swap all fee token balance to BNB

Additional information: Contract can swap all fee token balance to BNB, this can cause a dump when variable "swapEnabled" is true and the token balance in the contract is large.

```
uint256 contractTokenBalance = balanceOf(address(this));
if (
    !inSwap &&
    from != uniswapV2Pair &&
    swapEnabled &&
    contractTokenBalance > 0
) {
    swapTokensForEth(contractTokenBalance);
    uint256 contractETHBalance = address(this).balance;
    if (contractETHBalance > 0) {
        sendETHToFee(address(this).balance);
    }
}
```

Recommendation

Swap a certain amount of tokens slowly and cannot be more than 0.5% of total supply

● **Low-Risk:** Could be fixed, will not bring problems.

Several functions are declared public, but are never called internally:

```
rescureForeignToken, setNewDevAddress, setNewMarketingAddress, setFee, toggleSwap,
excludeMultipleAccountsFromFees
```

Recommendation

These functions should be declared external for additional gas savings on each call.

● **Low-Risk:** Could be fixed, will not bring problems.

No zero address validation for some functions

Detect missing zero address validation.

```
function setNewDevAddress(address payable dev) public onlyDev {
    emit devAddressUpdated(_developmentAddress, dev);
    _developmentAddress = dev;
    _isExcludedFromFee[_developmentAddress] = true;
}
function setNewMarketingAddress(address payable markt) public onlyDev {
    emit marketingAddressUpdated(_marketingAddress, markt);
    _marketingAddress = markt;
    _isExcludedFromFee[_marketingAddress] = true;
}
```

Recommendation

Check that the new address is not zero.

Exploit scenario

```
contract C {

    modifier onlyAdmin {
        if (msg.sender != owner) throw;
        _;
    }










    function updateOwner(address newOwner) onlyAdmin external {
        owner = newOwner;
    }
}
```

Bob calls updateOwner without specifying the newOwner, so Bob loses ownership of the contract.

Vulnerability Checklist

Nº	Description.	Result
1	Compiler warnings.	Passed
2	Race conditions and Re-entrancy. Cross-function race	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Zeppelin module.	Passed
21	Fallback function security.	Passed

Contract overview

-  KYC verified by ApeSale
-  Owner cannot set fees buy to 7%, sell to 11%
-  Owner cannot pause trading
-  Owner cannot change max transaction amount
-  No burn functions are present though the circulating supply can be decreased by sending tokens to the 0x..dead address.
-  At the time of writing this report, 100% of the total supply belongs to ApeSale presale.
-  The owner can set each fee to any value as long as the total fee percentage combined does not exceed 11% on sell.
-  The owner can exclude accounts from transfer fees.
-  The owner can withdraw any BNB or tokens from the contract at any time.

WORKOUT

Audited by ApeSale.app



APESALE

Date: 9 Jun 2022

✓ Advanced Manual Smart Contract Audit