



APE SALE

Smart Contract Security Audit



Project: RatsCoinV2

Website: <https://rat2coin.com/>



Low-Risk

1 low-risk code
issues found



Medium-Risk

0 medium-risk code
issue found



High-Risk

0 high-risk code issue
found

Contract Address

0xac2653Eb7C04403826C2c6f83866b11cd368189f

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)
1	0xac2653Eb7C04403826C2c6f83866b11cd368189f	10,000,000

Source Code

ApeSale was commissioned by RatsCoinV2 to perform an audit based on the following smart contract:

<https://bscscan.com/address/0xac2653Eb7C04403826C2c6f83866b11cd368189f#cod>

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

No zero address validation for some functions

Detect missing zero address validation.

```
function changeMarketingWallet(address _marketingWallet)
    external
    onlyOwner
{
    require(
        _marketingWallet != marketingWallet,
        "Marketing wallet is already that address"
    );
    require(
        !isContract(_marketingWallet),
        "Marketing wallet cannot be a contract"
    );
    marketingWallet = _marketingWallet;
    emit MarketingWalletChanged(marketingWallet);
}
```

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.

aph

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

Contract overview

-  Owner can set fees buy to 25%, sell to 25%
-  Not a contract upgradable
-  Owner cannot mint
-  Owner cannot pause trading
-  No burn functions are present though the circulating supply can be decreased by sending tokens to the 0x..dead address.
-  There is a Marketing fee on all transfers via Pancakeswap where neither the sender nor the recipient is excluded from fees

KANGUINU

Audited by ApeSale.app



APESALE

Date: 11 Jul 2022

✓ Advanced Manual Smart Contract Audit