



Cyberscope

Audit Report

YakuzaBoss

February 2023

SHA256

54eba09c54882d19d9363ddc5aee4d46545e0cba8ea83b7ba346f58ec3bbd106

Audited by © cyberscope

Table of Contents

| | |
|--|-----------|
| Table of Contents | 1 |
| Review | 1 |
| Audit Updates | 2 |
| Source Files | 2 |
| Analysis | 2 |
| Diagnostics | 3 |
| PR - Potential Reentrance | 4 |
| Description | 4 |
| Recommendation | 5 |
| L04 - Conformance to Solidity Naming Conventions | 5 |
| Description | 6 |
| Recommendation | 7 |
| L07 - Missing Events Arithmetic | 7 |
| Description | 7 |
| Recommendation | 8 |
| L12 - Using Variables before Declaration | 8 |
| Description | 8 |
| Recommendation | 9 |
| L14 - Uninitialized Variables in Local Scope | 9 |
| Description | 10 |
| Recommendation | 10 |
| L16 - Validate Variable Setters | 10 |
| Description | 10 |
| Recommendation | 11 |
| L20 - Succeeded Transfer Check | 11 |
| Description | 11 |
| Recommendation | 12 |
| Functions Analysis | 12 |
| Inheritance Graph | 16 |
| Flow Graph | 16 |
| Summary | 16 |
| Disclaimer | 19 |
| About Cyberscope | 20 |

Review

| | |
|------------------|---|
| Contract Name | YakuzaBoss |
| Compiler Version | v0.8.11+commit.d7f03943 |
| Optimization | 200 runs |
| Explorer | https://testnet.bscscan.com/address/0x07d4fc73b2a1cd1d46b3f7b461150dfa72d7ae0a |
| Address | 0x07d4fc73b2a1cd1d46b3f7b461150dfa72d7ae0a |
| Network | BSC_TESTNET |
| Symbol | BOSS |
| Decimals | 18 |
| Total Supply | 100,000,000 |

Audit Updates

| | |
|---------------|-------------|
| Initial Audit | 28 Feb 2023 |
|---------------|-------------|

Source Files

| | |
|--------------------------|--|
| Filename | SHA256 |
| contracts/YakuzaBoss.sol | 54eba09c54882d19d9363ddc5aee4d46545e0cba8ea83b7ba346f58ec3bbd106 |

Analysis

● Critical ● Medium ● Minor / Informative ● Pass

| Severity | Code | Description | Status |
|----------|------|------------------------------------|--------|
| ● | ST | Stops Transactions | Passed |
| ● | OCTD | Transfers Contract's Tokens | Passed |
| ● | OTUT | Transfers User's Tokens | Passed |
| ● | ELFM | Exceeds Fees Limit | Passed |
| ● | ULTW | Transfers Liquidity to Team Wallet | Passed |
| ● | MT | Mints Tokens | Passed |
| ● | BT | Burns Tokens | Passed |
| ● | BC | Blacklists Addresses | Passed |

Diagnostics

● Critical ● Medium ● Minor / Informative

| Severity | Code | Description | Status |
|----------|------|--|------------|
| ● | PR | Potential Reentrance | Unresolved |
| ● | L04 | Conformance to Solidity Naming Conventions | Unresolved |
| ● | L07 | Missing Events Arithmetic | Unresolved |
| ● | L12 | Using Variables before Declaration | Unresolved |
| ● | L14 | Uninitialized Variables in Local Scope | Unresolved |
| ● | L16 | Validate Variable Setters | Unresolved |
| ● | L20 | Succeeded Transfer Check | Unresolved |

PR - Potential Reentrance

| | |
|-------------|-------------------------------|
| Criticality | Minor / Informative |
| Location | contracts/YakuzaBoss.sol#L608 |
| Status | Unresolved |

Description

As part of the `swap` method, the contract transfers ETH to the latest user that buys more than a specific amount of tokens. Since the recipient can be any address, the address can be exploited for a re-entrance attack. The user will still have the entire balance during the re-entrance phase since the amount has not yet been subtracted.

```
if (ratios.yakuza > 0 && !entry) {
    entry = true;
    (success,) = _taxWallets.currentYakuzaBoss.call{value: yakuzaBalance, gas:
26000}("");
    if (success) {
        totalTributeReceived[_taxWallets.currentYakuzaBoss] += yakuzaBalance;
    }
    entry = false;
}
```

Recommendation

The team is advised to prevent the re-entrance exploit as part of the solidity best practices. Some suggestions are:

- Not allow contract addresses to receive funds.
- Add a locker/mutex in the transfer method scope.
- Transfer the funds as the last statement of the transfer method, so that the balance will have been subtracted during the re-entrance phase.

L04 - Conformance to Solidity Naming Conventions

| | |
|--------------------|--|
| Criticality | Minor / Informative |
| Location | contracts/YakuzaBoss.sol#L33,116,117,118,119,120,134,140,146,147,148,149,161,173,428 |
| Status | Unresolved |

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
function WETH() external pure returns (address);
uint256 constant private startingSupply = 100_000_000
string constant private _name = "Yakuza Boss"
string constant private _symbol = "BOSS"
uint8 constant private _decimals = 18
uint256 constant private _tTotal = startingSupply * 10**_decimals

Fees public _taxRates = Fees({
    buyFee: 500,
    sellFee: 500,
    transferFee: 0
})

...
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.

Find more information on the Solidity documentation

<https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention>.

L07 - Missing Events Arithmetic

| | |
|--------------------|---------------------------------------|
| Criticality | Minor / Informative |
| Location | contracts/YakuzaBoss.sol#L466,476,490 |
| Status | Unresolved |

Description

Events are a way to record and log information about changes or actions that occur within a contract. They are often used to notify external parties or clients about events that have occurred within the contract, such as the transfer of tokens or the completion of a task.

It's important to carefully design and implement the events in a contract, and to ensure that all required events are included. It's also a good idea to test the contract to ensure that all events are being properly triggered and logged.

```
swapThreshold = (_tTotal * thresholdPercent) / thresholdDivisor
piSwapPercent = priceImpactSwapPercent
minimumTribute = amountInTokens * 10**_decimals
```

Recommendation

By including all required events in the contract and thoroughly testing the contract's functionality, the contract ensures that it performs as intended and does not have any missing events that could cause issues with its arithmetic.

L12 - Using Variables before Declaration

| | |
|--------------------|-----------------------------------|
| Criticality | Minor / Informative |
| Location | contracts/YakuzaBoss.sol#L639,671 |
| Status | Unresolved |

Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or if the variable has been declared in a different scope. It is not a good practice to use a local variable before it has been declared.

```
uint256 initThreshold  
uint256 initSwapAmount  
bool check
```

Recommendation

By declaring local variables before using them, contract ensures that it operates correctly. It's important to be aware of this rule when working with local variables, as using a variable before it has been declared can lead to unexpected behavior and can be difficult to debug.

L14 - Uninitialized Variables in Local Scope

| | |
|--------------------|---------------------------------------|
| Criticality | Minor / Informative |
| Location | contracts/YakuzaBoss.sol#L639,670,671 |
| Status | Unresolved |

Description

Using an uninitialized local variable can lead to unpredictable behavior and potentially cause errors in the contract. It's important to always initialize local variables with appropriate values before using them.

```
uint256 initSwapAmount  
uint256 initThreshold  
bool checked  
bool check
```

Recommendation

By initializing local variables before using them, the contract ensures that the functions behave as expected and avoid potential issues.

L16 - Validate Variable Setters

| | |
|--------------------|-------------------------------|
| Criticality | Minor / Informative |
| Location | contracts/YakuzaBoss.sol#L279 |
| Status | Unresolved |

Description

The contract performs operations on variables that have been configured on user-supplied input. These variables are missing of proper check for the case where a value is zero. This can lead to problems when the contract is executed, as certain actions may not be properly handled when the value is zero.

```
operator = newOperator
```

Recommendation

By adding the proper check, the contract will not allow the variables to be configured with zero value. This will ensure that the contract can handle all possible input values and avoid unexpected behavior or errors. Hence, it can help to prevent the contract from being exploited or operating unexpectedly.

L20 - Succeeded Transfer Check

| | |
|--------------------|-------------------------------|
| Criticality | Minor / Informative |
| Location | contracts/YakuzaBoss.sol#L658 |
| Status | Unresolved |

Description

According to the ERC20 specification, the transfer methods should be checked if the result is successful. Otherwise, the contract may wrongly assume that the transfer has been established.

```
TOKEN.transfer(_owner, TOKEN.balanceOf(address(this)))
```

Recommendation

The contract should check if the result of the transfer methods is successful. The team is advised to check the SafeERC20 library from the [Openzeppelin library](#).

Functions Analysis

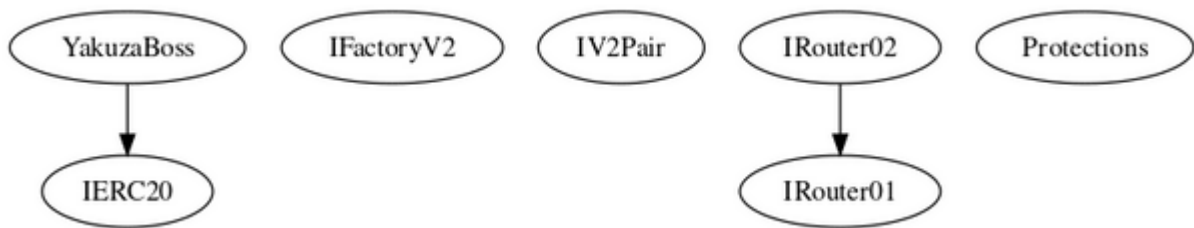
| Contract | Type | Bases | | |
|------------|---------------|------------|------------|-----------|
| | Function Name | Visibility | Mutability | Modifiers |
| IERC20 | Interface | | | |
| | totalSupply | External | | - |
| | decimals | External | | - |
| | symbol | External | | - |
| | name | External | | - |
| | getOwner | External | | - |
| | balanceOf | External | | - |
| | transfer | External | ✓ | - |
| | allowance | External | | - |
| | approve | External | ✓ | - |
| | transferFrom | External | ✓ | - |
| | | | | |
| IFactoryV2 | Interface | | | |
| | getPair | External | | - |
| | createPair | External | ✓ | - |
| | | | | |
| IV2Pair | Interface | | | |
| | factory | External | | - |
| | getReserves | External | | - |
| | sync | External | ✓ | - |
| | | | | |
| IRouter01 | Interface | | | |
| | factory | External | | - |
| | WETH | External | | - |

| | | | | |
|--------------------|---|-----------|---------|-----------|
| | addLiquidityETH | External | Payable | - |
| | addLiquidity | External | ✓ | - |
| | swapExactETHForTokens | External | Payable | - |
| | getAmountsOut | External | | - |
| | getAmountsIn | External | | - |
| | | | | |
| IRouter02 | Interface | IRouter01 | | |
| | swapExactTokensForETHSupporting FeeOnTransferTokens | External | ✓ | - |
| | swapExactETHForTokensSupporting FeeOnTransferTokens | External | Payable | - |
| | swapExactTokensForTokensSupporti ngFeeOnTransferTokens | External | ✓ | - |
| | swapExactTokensForTokens | External | ✓ | - |
| | | | | |
| Protections | Interface | | | |
| | checkUser | External | ✓ | - |
| | setLaunch | External | ✓ | - |
| | getInits | External | ✓ | - |
| | setLpPair | External | ✓ | - |
| | setProtections | External | ✓ | - |
| | removeSniper | External | ✓ | - |
| | isBlacklisted | External | | - |
| | setBlacklistEnabled | External | ✓ | - |
| | setBlacklistEnabledMultiple | External | ✓ | - |
| | removeBlacklisted | External | ✓ | - |
| | | | | |
| YakuzaBoss | Implementation | IERC20 | | |
| | | Public | Payable | - |
| | transferOwner | External | ✓ | onlyOwner |
| | renounceOwnership | External | ✓ | onlyOwner |

| | | | | |
|--|-----------------------------|----------|---------|-----------|
| | setOperator | Public | ✓ | - |
| | renounceOriginalDeployer | External | ✓ | - |
| | | External | Payable | - |
| | totalSupply | External | | - |
| | decimals | External | | - |
| | symbol | External | | - |
| | name | External | | - |
| | getOwner | External | | - |
| | allowance | External | | - |
| | balanceOf | Public | | - |
| | transfer | Public | ✓ | - |
| | approve | External | ✓ | - |
| | _approve | Internal | ✓ | |
| | approveContractContingency | External | ✓ | onlyOwner |
| | transferFrom | External | ✓ | - |
| | setNewRouter | External | ✓ | onlyOwner |
| | setLpPair | External | ✓ | onlyOwner |
| | setInitializer | External | ✓ | onlyOwner |
| | isExcludedFromLimits | External | | - |
| | setExcludedFromLimits | External | ✓ | onlyOwner |
| | isExcludedFromFees | External | | - |
| | setExcludedFromFees | Public | ✓ | onlyOwner |
| | isExcludedFromProtection | External | | - |
| | setExcludedFromProtection | External | ✓ | onlyOwner |
| | getCirculatingSupply | Public | | - |
| | setBlacklistEnabled | External | ✓ | - |
| | setBlacklistEnabledMultiple | External | ✓ | - |
| | isBlacklisted | External | | - |
| | removeBlacklisted | External | ✓ | onlyOwner |

| | | | | |
|--|-----------------------------|----------|---|------------|
| | removeSniper | External | ✓ | onlyOwner |
| | setProtectionSettings | External | ✓ | onlyOwner |
| | lockTaxes | External | ✓ | onlyOwner |
| | setTaxes | External | ✓ | onlyOwner |
| | setRatios | External | ✓ | onlyOwner |
| | setWallets | External | ✓ | onlyOwner |
| | getTokenAmountAtPriceImpact | External | | - |
| | setSwapSettings | External | ✓ | onlyOwner |
| | setPriceImpactSwapAmount | External | ✓ | onlyOwner |
| | setContractSwapEnabled | External | ✓ | onlyOwner |
| | setYakuzaEnabled | External | ✓ | onlyOwner |
| | setMinimumTribute | External | ✓ | onlyOwner |
| | getMinimumTribute | External | | - |
| | getTotalTributeReceived | External | | - |
| | excludePresaleAddresses | External | ✓ | onlyOwner |
| | _hasLimits | Internal | | |
| | _transfer | Internal | ✓ | |
| | contractSwap | Internal | ✓ | inSwapFlag |
| | _checkLiquidityAdd | Internal | ✓ | |
| | enableTrading | Public | ✓ | onlyOwner |
| | sweepContingency | External | ✓ | onlyOwner |
| | sweepExternalTokens | External | ✓ | onlyOwner |
| | multiSendTokens | External | ✓ | onlyOwner |
| | finalizeTransfer | Internal | ✓ | |
| | takeTaxes | Internal | ✓ | |

Inheritance Graph



Flow Graph

Summary

Yakuza Boss contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. Yakuza Boss is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler errors or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 10% buy, sell, and transfer fees.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security. Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.



The Cyberscope team

<https://www.cyberscope.io>