

ContractCenter Audit Report

Arcaida Token

Contract Address : 0x86a599ED3cC627E109324DDb53CE57d20ee82ae8

Total Supply: 5 000 000

Auditor: t.me/AnanCoder

Source Code SHA256 Hash:

9e04d3b26cac850b1ff1a4081b5bd4d8ba7ba85a253f0040b7040b8d94e3fc04

Compiler version : ^0.8.0

Audit Type : Manual

● Critical:

Line 787 | function addTax

Issue:

this function is supposed to change both buy and sell taxes, but taxes get overridden by setting in lines 794-798

recommendation:

create two mappings for buy taxes and sell taxes or change TaxInfo storage sellTax = taxes[nthDay][true] to TaxInfo storage sellTax = taxes[nthDay][false];

● Critical:

Line 800 | function setTax

Issue:

this function is supposed to change both buy and sell taxes, but taxes get overridden by setting in lines 807-8011

it must be

recommendation:

create two mappings for buy taxes and sell taxes or change TaxInfo storage sellTax = taxes[nthDay][true] to TaxInfo storage sellTax = taxes[nthDay][false];

◆ Major

line 855 | getTaxInfo

Issue:

if period (a variable in contract) is passed, then n2 will be:

$86400 * (\text{block.timestamp} - \text{whenAppliedTax}) / \text{period}$, hence, **n2** will be a much much bigger value than

lastDay and getTaxInfo will always return taxes[lastDay][forWhat]

recommendation:

It is unclear what the purpose behind **nthDay** and **lastDay**. We recommend you to override this function just to return taxes using lastDay value and terminate nthDay from contract.

♦ Major

if whenAppliedTax == false => there wont be any transfers allowed. even for whitelisted wallets

recommendations:

- give permission to owner for transferring tokens even when this variable is false
 - make two seperate variables, one for tax status and another one for transferring status, whitelist admins from all of these conditions
-

♦ Major

line 872 | _transfer

there are a couple of issues in this function:

- 1- blacklisted users can sell their tokens.
- 2- the owner is not excluded from the second condition(which requires appliedTax to be true)
- 3- there is not a tax denominator variable (used 1e4)

recommendations:

- check if both "to" and "from" are not blacklisted
 - exclude owner and other whitelisted wallets from all conditions
 - create a tax denominator variable. You may want to change the tax scale later
-

♦ Minimal

you are not excluding deployer from taxes in constructor

♦ Minimal

Emit an event when taxes gets changed at setTax and addTax functions

♦ Minimal

functions setIP, setWhitelist, setVault, setMarket, setDeveloper, setBlacklist

this function is not checking whether the given address is address(0) or not.

recommendation:

add a require statement that reverts if the given address is address(0)

♦ Information

create a totalFees variable to keep track of all fees

♦ Information

Contract has receive function, make a withdraw function to withdraw contract ETH balance

♦ Information

you excluded developer from taxes two times in constructore

```
whitelistTax[developer] = true;
```

```
whitelistTax[developer] = true;
```

About us

- ◆ Telegram : t.me/ContractCenter
- ◆ Website : <https://contractcenter.xyz>
- ◆ Owner : t.me/AnanCoder