SmartDec

KaratGold Smart Contracts Security Analysis

This report is public.

Published: June 22, 2018

Abstract

In this report, we consider the security of the KaratGold project. Our task is to find and describe security issues in the smart contracts of the platform.

Disclaimer

The audit does not give any warranties on the security of the code. One audit cannot be considered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. Besides, security audit is not an investment advice.

Summary

In this report, we have considered the security of KaratGold smart contracts. We performed our audit according to the procedure described below.

The audit has shown neither critical nor medium severity issues. However, a number of low severity issues were found.

The token contract has already been deployed. The issues found during the audit do not endanger the project security.

General recommendations

The contracts code is of good code quality and does not contain issues that endanger project security. However, we would recommend completing the Documentation and informing users about ERC20 approve issue.

In addition, if the developers decide to improve the code, we would recommend following the best practices for Pragmas and OpenZeppelin versions, removing Redundant code and Deprecated constructions, and marking Visibility explicitly.

However, these are minor issues, which do not influence code operation.

The text below is for technical use; it details the statements made in Summary and General recommendations.

Procedure

In our audit, we consider the following crucial features of the smart contract code:

1. Whether the code is secure.
2. Whether the code corresponds to the documentation (including whitepaper).
3. Whether the code meets best practices in efficient use of gas, code readability, etc.

We perform our audit according to the following procedure:

- automated analysis
  - we scan project's smart contracts with our own Solidity static code analyzer SmartCheck
  - we scan project's smart contracts with several publicly available automated Solidity analysis tools such as Remix, Oyente, and Solhint
  - we manually verify (reject or confirm) all the issues found by tools
- manual audit
  - we manually analyze smart contracts for security vulnerabilities
  - we check smart contracts logic and compare it with the one described in the whitepaper
  - we check ERC20 compliance
- report
  - we reflect all the gathered information in the report

Checked vulnerabilities

We have scanned KaratGold smart contracts for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered (the full list includes them but is not limited to them):

- Reentrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with (Unexpected) Throw
- DoS with (Unexpected) revert
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level
- Address hardcoded
- Using delete for arrays
- Integer overflow/underflow
- Locked money
- Private modifier
- Revert/require functions
- Using var
- Visibility
- Using blockhash
- Using SHA3
- Using suicide
- Using throw
- Using inline assembly

Project overview

Project description

In our analysis, we have considered KaratGold whitepaper (“karatgold-wp.pdf”, sha1sum 9b24a6ab833ddb721e8f35dd9471b49a84e9cfb2) and smart contracts code.

Project architecture

For the audit, we have been provided with the smart contracts code.

- The code successfully compiles with `solcjs` command (with some warnings, see Compilation output in Appendix)

The provided code contains the following contracts from OpenZeppelin library with some minor modifications:

- **ERC20Basic**
- **ERC20**
- **BasicToken**
- **StandardToken**
- **Ownable**

The following contracts implement additional features for the token:

- **InvestorsFeature** (inherits **Ownable** and **StandardToken** contracts)
- **KaratBankCoin** (inherits **Ownable**, **StandardToken**, and **InvestorsFeature** contracts)

The total volume of audited Solidity code is 142 lines.

Code logic

KaratBankCoin is ERC20 compatible (compatibility has been checked during the audit) token contract with the following parameters:

- token name: “KaratBank Coin”
- token symbol: “KBC”
- token decimals: 7
- the initial supply: 12 000 000 000 tokens

Besides, some additional functionality is implemented:

1. The contract inherits **Ownable** contract. This means that the contract has an owner (initially, it is the address the contract was deployed from).
2. The contract includes `increaseApproval()` and `decreaseApproval()` functions. This makes changing the `allowance` mapping possible without using `approve()` function, which has a vulnerability (see ERC20 approve issue).
3. At the moment of deploy all the tokens are transferred to the token contract address.

The contract includes some additional functions:

```
function send(address addr, uint amount)
```

- Call restrictions: only owner can call the function
- Parameters requirements:
    - `addr` address is not null
    - `amount` is positive
- Logic:
    - puts every unique `addr` address in the `investors` array, which is publicly available
    - transfers `amount` of tokens from the token contract address to `addr` address

```
function moneyBack(address addr)
```

- Call restrictions: only owner can call the function
- Parameters requirements:
    - `addr` address is not null
- Logic: transfers all the ETH from the token contract address to `addr` address

```
function burnRemainder(uint)
```

- Call restrictions: only owner can call the function
- Logic: burns all the tokens from the token contract address

Automated analysis

We used several publicly available automated Solidity analysis tools. Here are the combined results of SmartCheck, Solhint, and Remix. Oyente has found no issues.
All the issues found by tools were manually checked (rejected or confirmed).

False positives are constructions that were discovered by the tools as vulnerabilities but do not consist a security threat.

True positives are constructions that were discovered by the tools as vulnerabilities and can actually be exploited by attackers or lead to incorrect contracts operation.

Cases when these issues lead to actual bugs or vulnerabilities are described in the next section.

Tool	Rule	False positives	True positives
Remix	Gas requirement of function high	18	
	Variables have very similar names	3	
Total Remix		21	
SmartCheck	Constant Functions		4
	Erc20 Approve		1
	No Payable Fallback	7	
	Pragmas Version		1
	Reentrancy External Call	6	
	Unchecked Math	1	
	Visibility		2
Total SmartCheck		14	8

Solhint	Compiler version must be fixed		1
	Explicitly mark visibility of state		2
Total Solhint			3
Total Overall		**35**	**11**

Manual analysis

The contracts were completely manually analyzed, their logic was checked and compared with the one described in the documentation. Besides, the results of the automated analysis were manually verified. All confirmed issues are described below.

Critical issues

Critical issues seriously endanger smart contracts security. We highly recommend fixing them.

The audit has shown no critical issues.

Medium severity issues

Medium issues can influence smart contracts operation in current implementation. We highly recommend addressing them.

The audit has shown no medium severity issues.

Low severity issues

Low severity issues can influence smart contracts operation in future versions of code. We recommend taking them into account.

Redundant code

The following lines include redundant code:

1. line 225:

```
function deposit(address investor, uint) internal {
```

The second argument in this function is redundant.

2. line 275:

```
function burnRemainder(uint) public onlyOwner {
```

The argument in this function is redundant.

We highly recommend removing redundant code in order to improve code readability.

Deprecated constructions

Deprecated syntax is used in some places in the code:

- `this.balance` is deprecated.
  However, the mentioned construction is used in the code, line 272:

  ```
  addr.transfer(this.balance);
  ```

  We recommend using `address(this).balance`.

- `constant` modifier for functions is deprecated. However, our audit has shown the use of `constant` modifier for functions in the following places:
  - line 41:

  ```
  function balanceOf(address who) public constant returns
  (uint256);
  ```

  - line 51:

  ```
  function allowance(address owner, address spender) public
  constant returns (uint256);
  ```

  - line 88:

  ```
  function balanceOf(address _owner) public constant returns
  (uint256 balance) {
  ```

  - line 146:

  ```
  function allowance(address _owner, address _spender) public
  constant returns (uint256 remaining) {
  ```

  We recommend using `view` instead of `constant`, since it will be deprecated for functions in compiler version 0.5.0.

- Invoking events without `emit` prefix is deprecated. However, `emit` prefix is not used in the following lines:
  - line 261:

  ```
  Transfer(address(0), this, INITIAL_SUPPLY);
  ```

  - line 240:

  ```
  Transfer(this, addr, amount);
  ```

- Defining constructor as function of the same name as the contract is deprecated. However, the constructor of the **KaratBankCoin** contract is implemented in the following way:

```
function KaratBankCoin() public {
```

We highly recommend not using deprecated constructions and following the best practices instead.

Using outdated library

The version of OpenZeppelin library used in the code is outdated. The contracts inherited in the token contract include deprecated constructions and some redundant code.
We recommend using the latest available version of OpenZeppelin library in case developer wants to redeploy the token contract.

Pragmas version

Solidity source files indicate the versions of the compiler they can be compiled with.
Example:

```
pragma solidity ^0.4.13; // bad: compiles w 0.4.13 and above
pragma solidity 0.4.13; // good: compiles w 0.4.13 only
```

We recommend following the latter example, as future compiler versions may handle certain language constructions in a way the developer did not foresee. Besides, we recommend using the latest compiler version – 0.4.24 at the moment.

Implicit visibility level

There are two state variables with implicit visibility level in the code:

- line 65:

```
mapping(address => uint256) balances;
```

- line 224:

```
mapping(address => bool) isInvestor;
```

We recommend specifying visibility levels (`public`, `private`, `external`, `internal`) explicitly and correctly in order to improve code readability.

Notes

ERC20 approve issue

There is ERC20 approve issue: changing the approved amount from a nonzero value to another nonzero value allows a double spending with a front-running attack.

We recommend instructing users to follow one of two ways:

- not to use `approve()` function directly and to use `increaseApproval()/decreaseApproval()` functions instead
- to change the approved amount to 0, wait for the transaction to be mined, and then to change the approved amount to the desired value

Lack of the documentation

According to the whitepaper, ICO has already finished. The information regarding unsold tokens (about 7 000 000 000 KBC at the moment of audit) is not specified in the documentation.
Currently, all the unsold tokens are assigned to the token contract address, including tokens reserved for partners, referrals, etc. Therefore, tokens can be burned or transferred to any address without any restrictions.
We recommend completing the documentation by adding the relevant information.

This analysis was performed by SmartDec.

Ivan Ivanitskiy, Chief Analytics Officer
Alexander Seleznev, Chief Business Development Officer
Igor Sobolev, Analyst
Pavel Kondratenkov, Analyst

Sergey Pavlin, Chief Operating Officer Pavli

June 22, 2018

Appendix

Compilation output

```
   192:3: Warning: Defining constructors as functions with the same
name as the contract is deprecated. Use "constructor(...) { ... }"
instead.
     function Ownable() public {
     ^ (Relevant source part starts here and spans across multiple
lines).

   258:3: Warning: Defining constructors as functions with the same
name as the contract is deprecated. Use "constructor(...) { ... }"
instead.
     function KaratBankCoin() public {
     ^ (Relevant source part starts here and spans across multiple
lines).

   79:5: Warning: Invoking events without "emit" prefix is
deprecated.
       Transfer(msg.sender, _to, _value);
       ^-------------------------------^

   120:5: Warning: Invoking events without "emit" prefix is
deprecated.
       Transfer(_from, _to, _value);
       ^--------------------------^

   136:5: Warning: Invoking events without "emit" prefix is
deprecated.
       Approval(msg.sender, _spender, _value);
       ^------------------------------------^

   158:5: Warning: Invoking events without "emit" prefix is
deprecated.
       Approval(msg.sender, _spender,
allowed[msg.sender][_spender]);
       ^-----------------------------------------------------------^

   169:5: Warning: Invoking events without "emit" prefix is
deprecated.
       Approval(msg.sender, _spender,
allowed[msg.sender][_spender]);
```

```
       ^-----------------------------------------------------------^

   212:5: Warning: Invoking events without "emit" prefix is
deprecated.
       OwnershipTransferred(owner, newOwner);
       ^-----------------------------------^

   240:9: Warning: Invoking events without "emit" prefix is
deprecated.
           Transfer(this, addr, amount);
           ^--------------------------^

   261:5: Warning: Invoking events without "emit" prefix is
deprecated.
       Transfer(address(0), this, INITIAL_SUPPLY);
       ^----------------------------------------^

   272:21: Warning: Using contract member "balance" inherited from
the address type is deprecated. Convert the contract to "address"
type to access the member, for example use
"address(contract).balance" instead.
         addr.transfer(this.balance);
                       ^----------^
```

Solhint output

```
    1:17  warning  Compiler version must be
fixed                                                          compi
ler-fixed
    7:1   error    Definition must be surrounded with two blank line
indent                                two-lines-top-level-separator
    8:3   error    Expected indentation of 4 spaces but found
2                                            indent
    9:5   error    Expected indentation of 8 spaces but found
4                                            indent
   10:5   error    Expected indentation of 8 spaces but found
4                                            indent
   11:5   error    Expected indentation of 8 spaces but found
4                                            indent
   12:3   error    Expected indentation of 4 spaces but found
2                                            indent
   14:3   error    Expected indentation of 4 spaces but found
2                                            indent
```

```
   16:5   error    Expected indentation of 8 spaces but found
4                                            indent
   18:5   error    Expected indentation of 8 spaces but found
4                                            indent
   19:3   error    Expected indentation of 4 spaces but found
2                                            indent
   21:3   error    Expected indentation of 4 spaces but found
2                                            indent
   22:5   error    Expected indentation of 8 spaces but found
4                                            indent
   23:5   error    Expected indentation of 8 spaces but found
4                                            indent
   24:3   error    Expected indentation of 4 spaces but found
2                                            indent
   26:3   error    Expected indentation of 4 spaces but found
2                                            indent
   27:5   error    Expected indentation of 8 spaces but found
4                                            indent
   28:5   error    Expected indentation of 8 spaces but found
4                                            indent
   29:5   error    Expected indentation of 8 spaces but found
4                                            indent
   30:3   error    Expected indentation of 4 spaces but found
2                                            indent
   39:1   error    Definition must be surrounded with two blank line
indent                                two-lines-top-level-separator
   40:3   error    Expected indentation of 4 spaces but found
2                                            indent
   41:3   error    Expected indentation of 4 spaces but found
2                                            indent
   42:3   error    Expected indentation of 4 spaces but found
2                                            indent
   43:3   warning  Event and function names must be
different                                              no-simple-
event-func-name
   43:3   error    Expected indentation of 4 spaces but found
2                                            indent
   50:1   error    Definition must be surrounded with two blank line
indent                                two-lines-top-level-separator
   51:3   error    Expected indentation of 4 spaces but found
2                                            indent
   52:3   error    Expected indentation of 4 spaces but found
2                                            indent
   53:3   error    Expected indentation of 4 spaces but found
2                                            indent
   54:3   error    Expected indentation of 4 spaces but found
2                                            indent
```

```
   62:1   error    Definition must be surrounded with two blank line
indent                                two-lines-top-level-separator
   63:3   error    Expected indentation of 4 spaces but found
2                                            indent
   65:3   error    Expected indentation of 4 spaces but found
2                                            indent
   65:3   warning  Explicitly mark visibility of
state                                                     state-
visibility
   72:3   warning  Event and function names must be
different                                              no-simple-
event-func-name
   72:3   error    Expected indentation of 4 spaces but found
2                                            indent
   73:5   error    Expected indentation of 8 spaces but found
4                                            indent
   74:5   error    Expected indentation of 8 spaces but found
4                                            indent
   77:5   error    Expected indentation of 8 spaces but found
4                                            indent
   78:5   error    Expected indentation of 8 spaces but found
4                                            indent
   79:5   error    Expected indentation of 8 spaces but found
4                                            indent
   80:5   error    Expected indentation of 8 spaces but found
4                                            indent
   81:3   error    Expected indentation of 4 spaces but found
2                                            indent
   88:3   error    Expected indentation of 4 spaces but found
2                                            indent
   89:5   error    Expected indentation of 8 spaces but found
4                                            indent
   90:3   error    Expected indentation of 4 spaces but found
2                                            indent
   99:2   error    Line length must be no more than 120 but current
length is 122                          max-line-length
  101:1   error    Definition must be surrounded with two blank line
indent                                two-lines-top-level-separator
  103:3   error    Expected indentation of 4 spaces but found
2                                            indent
  112:3   error    Definitions inside contract / library must be
separated by one line               separate-by-one-line-in-contract
  112:3   error    Expected indentation of 4 spaces but found
2                                            indent
  113:5   error    Expected indentation of 8 spaces but found
4                                            indent
```

```
  114:5   error    Expected indentation of 8 spaces but found
4                                            indent
  115:5   error    Expected indentation of 8 spaces but found
4                                            indent
  117:5   error    Expected indentation of 8 spaces but found
4                                            indent
  118:5   error    Expected indentation of 8 spaces but found
4                                            indent
  119:5   error    Expected indentation of 8 spaces but found
4                                            indent
  120:5   error    Expected indentation of 8 spaces but found
4                                            indent
  121:5   error    Expected indentation of 8 spaces but found
4                                            indent
  122:3   error    Expected indentation of 4 spaces but found
2                                            indent
  134:3   error    Expected indentation of 4 spaces but found
2                                            indent
  135:5   error    Expected indentation of 8 spaces but found
4                                            indent
  136:5   error    Expected indentation of 8 spaces but found
4                                            indent
  137:5   error    Expected indentation of 8 spaces but found
4                                            indent
  138:3   error    Expected indentation of 4 spaces but found
2                                            indent
  146:3   error    Expected indentation of 4 spaces but found
2                                            indent
  147:5   error    Expected indentation of 8 spaces but found
4                                            indent
  148:3   error    Expected indentation of 4 spaces but found
2                                            indent
  156:3   error    Expected indentation of 4 spaces but found
2                                            indent
  157:5   error    Expected indentation of 8 spaces but found
4                                            indent
  158:5   error    Expected indentation of 8 spaces but found
4                                            indent
  159:5   error    Expected indentation of 8 spaces but found
4                                            indent
  160:3   error    Expected indentation of 4 spaces but found
2                                            indent
  162:3   error    Expected indentation of 4 spaces but found
2                                            indent
  163:5   error    Expected indentation of 8 spaces but found
4                                            indent
```

```
  164:5   error    Expected indentation of 8 spaces but found
4                                            indent
  165:7   error    Expected indentation of 12 spaces but found
6                                           indent
  166:5   error    Expected indentation of 8 spaces but found
4                                            indent
  167:7   error    Expected indentation of 12 spaces but found
6                                           indent
  168:5   error    Expected indentation of 8 spaces but found
4                                            indent
  169:5   error    Expected indentation of 8 spaces but found
4                                            indent
  170:5   error    Expected indentation of 8 spaces but found
4                                            indent
  171:3   error    Expected indentation of 4 spaces but found
2                                            indent
  181:1   error    Definition must be surrounded with two blank line
indent                                 two-lines-top-level-separator
  182:3   error    Expected indentation of 4 spaces but found
2                                            indent
  185:3   error    Expected indentation of 4 spaces but found
2                                            indent
  192:3   error    Definitions inside contract / library must be
separated by one line               separate-by-one-line-in-contract
  192:3   error    Expected indentation of 4 spaces but found
2                                            indent
  193:5   error    Expected indentation of 8 spaces but found
4                                            indent
  194:3   error    Expected indentation of 4 spaces but found
2                                            indent
  200:3   error    Definitions inside contract / library must be
separated by one line               separate-by-one-line-in-contract
  200:3   error    Expected indentation of 4 spaces but found
2                                            indent
  201:5   error    Expected indentation of 8 spaces but found
4                                            indent
  202:5   error    Expected indentation of 8 spaces but found
4                                            indent
  203:3   error    Expected indentation of 4 spaces but found
2                                            indent
  210:3   error    Expected indentation of 4 spaces but found
2                                            indent
  210:3   error    Definitions inside contract / library must be
separated by one line               separate-by-one-line-in-contract
  211:5   error    Expected indentation of 8 spaces but found
4                                            indent
```

```
  212:5   error    Expected indentation of 8 spaces but found
4                                            indent
  213:5   error    Expected indentation of 8 spaces but found
4                                            indent
  214:3   error    Expected indentation of 4 spaces but found
2                                            indent
  220:1   error    Definition must be surrounded with two blank line
indent                                two-lines-top-level-separator
  224:5   warning  Explicitly mark visibility of
state                                                     state-
visibility
  225:5   error    Definitions inside contract / library must be
separated by one line              separate-by-one-line-in-contract
  226:9   error    Statement indentation is incorrect. Required
space after if                             statement-indent
  247:1   error    Definition must be surrounded with two blank line
indent                                two-lines-top-level-separator
  247:69  error    Open bracket must be on same line. It must be
indented by other constructions by space  bracket-align
  250:26  error    Constant name must be in capitalized
SNAKE_CASE                                         const-name-
snakecase
  250:3   error    Expected indentation of 4 spaces but found
2                                            indent
  251:3   error    Expected indentation of 4 spaces but found
2                                            indent
  251:26  error    Constant name must be in capitalized
SNAKE_CASE                                         const-name-
snakecase
  252:3   error    Expected indentation of 4 spaces but found
2                                            indent
  252:25  error    Constant name must be in capitalized
SNAKE_CASE                                         const-name-
snakecase
  254:3   error    Expected indentation of 4 spaces but found
2                                            indent
  258:3   error    Expected indentation of 4 spaces but found
2                                            indent
  258:3   error    Definitions inside contract / library must be
separated by one line               separate-by-one-line-in-contract
  259:5   error    Expected indentation of 8 spaces but found
4                                            indent
  260:5   error    Expected indentation of 8 spaces but found
4                                            indent
  261:5   error    Expected indentation of 8 spaces but found
4                                            indent
```

```
  262:3   error    Expected indentation of 4 spaces but found
2                                            indent
  266:3   error    Expected indentation of 4 spaces but found
2                                            indent
  266:3   error    Definitions inside contract / library must be
separated by one line               separate-by-one-line-in-contract
  267:7   error    Expected indentation of 8 spaces but found
6                                            indent
  268:3   error    Expected indentation of 4 spaces but found
2                                            indent
  270:3   error    Expected indentation of 4 spaces but found
2                                            indent
  271:7   error    Expected indentation of 8 spaces but found
6                                            indent
  272:7   error    Expected indentation of 8 spaces but found
6                                            indent
  273:3   error    Expected indentation of 4 spaces but found
2                                            indent
  275:3   error    Expected indentation of 4 spaces but found
2                                            indent
  276:7   error    Expected indentation of 8 spaces but found
6                                            indent
  277:7   error    Expected indentation of 8 spaces but found
6                                            indent
  278:7   error    Expected indentation of 8 spaces but found
6                                            indent
  279:3   error    Expected indentation of 4 spaces but found
2                                            indent

✕ 134 problems (129 errors, 5 warnings)
```

Solium output

```
  8:2       error      Only use indent of 4 spaces.      indentation
  12:0      error      Only use indent of 4 spaces.      indentation
  14:2      error      Only use indent of 4 spaces.      indentation
  19:0      error      Only use indent of 4 spaces.      indentation
  21:2      error      Only use indent of 4 spaces.      indentation
  24:0      error      Only use indent of 4 spaces.      indentation
  26:2      error      Only use indent of 4 spaces.      indentation
  30:0      error      Only use indent of 4 spaces.      indentation
  40:2      error      Only use indent of 4 spaces.      indentation
  41:2      error      Only use indent of 4 spaces.      indentation
  41:41     warning    Use 'view' instead of deprecated
```

```
'constant'.    no-constant
  42:2      error      Only use indent of 4 spaces.      indentation
  43:2      error      Only use indent of 4 spaces.      indentation
  51:2      error      Only use indent of 4 spaces.      indentation
  51:60     warning    Use 'view' instead of deprecated
'constant'.    no-constant
  52:2      error      Only use indent of 4 spaces.      indentation
  53:2      error      Only use indent of 4 spaces.      indentation
  54:2      error      Only use indent of 4 spaces.      indentation
  63:2      error      Only use indent of 4 spaces.      indentation
  65:2      error      Only use indent of 4 spaces.      indentation
  72:2      error      Only use indent of 4 spaces.      indentation
  81:0      error      Only use indent of 4 spaces.      indentation
  88:2      error      Only use indent of 4 spaces.      indentation
  88:44     warning    Use 'view' instead of deprecated
'constant'.    no-constant
  90:0      error      Only use indent of 4 spaces.      indentation
  103:2     error      Only use indent of 4 spaces.      indentation
  112:2     error      Only use indent of 4 spaces.      indentation
  122:0     error      Only use indent of 4 spaces.      indentation
  134:2     error      Only use indent of 4 spaces.      indentation
  138:0     error      Only use indent of 4 spaces.      indentation
  146:2     error      Only use indent of 4 spaces.      indentation
  146:62    warning    Use 'view' instead of deprecated
'constant'.    no-constant
  148:0     error      Only use indent of 4 spaces.      indentation
  156:2     error      Only use indent of 4 spaces.      indentation
  160:0     error      Only use indent of 4 spaces.      indentation
  162:2     error      Only use indent of 4 spaces.      indentation
  165:6     error      Only use indent of 8 spaces.      indentation
  167:6     error      Only use indent of 8 spaces.      indentation
  171:0     error      Only use indent of 4 spaces.      indentation
  182:2     error      Only use indent of 4 spaces.      indentation
  185:2     error      Only use indent of 4 spaces.      indentation
  192:2     error      Only use indent of 4 spaces.      indentation
  194:0     error      Only use indent of 4 spaces.      indentation
  200:2     error      Only use indent of 4 spaces.      indentation
  203:0     error      Only use indent of 4 spaces.      indentation
  210:2     error      Only use indent of 4 spaces.      indentation
  212:4     warning    Use emit statements for triggering
events.      emit
  214:0     error      Only use indent of 4 spaces.      indentation
  250:2     error      Only use indent of 4 spaces.      indentation
  251:2     error      Only use indent of 4 spaces.      indentation
  252:2     error      Only use indent of 4 spaces.      indentation
  254:2     error      Only use indent of 4 spaces.      indentation
  258:2     error      Only use indent of 4 spaces.      indentation
  262:0     error     Only use indent of 4 spaces.     indentation
  266:2     error     Only use indent of 4 spaces.     indentation
  268:0     error     Only use indent of 4 spaces.     indentation
  270:2     error     Only use indent of 4 spaces.     indentation
  273:0     error     Only use indent of 4 spaces.     indentation
  275:2     error     Only use indent of 4 spaces.     Indentation
  279:0     error     Only use indent of 4 spaces.     Indentation

✕ 55 errors, 5 warnings found.
```