MythX

Analysis 408d1f0a-4b3b-467f-bfa7-d562f7b58d09 MythX

| | |
|---|---|
| Started | Wed May 26 2021 20:02:36 GMT+0000 (Coordinated Universal Time) |
| Finished | Wed May 26 2021 20:48:41 GMT+0000 (Coordinated Universal Time) |
| Mode | Deep |
| Client Tool | Remythx |
| Main Source File | KangarooToken.Sol |

## DETECTED VULNERABILITIES

| HIGH | MEDIUM | LOW |
|---|---|---|
| 0 | 13 | 6 |

## ISSUES

MEDIUM Function could be marked as external.

SWC-000

The function definition of "mint" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

IBEP20.sol

Locations

```
10  * @dev Returns the token decimals.
11  */
12  function decimals() external view returns (uint8);
13
14  /**
15  * @dev Returns the token symbol.
16  */
17  function symbol() external view returns (string memory);
18
19  /**
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "symbol" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
60
61  /**
62  * @notice Delegate votes from `msg.sender` to `delegatee`
63  * @param delegatee The address to delegate votes to
64  */
65  function delegate(address delegatee) external {
66  function delegate(address delegatee) external {
67  return _delegate(msg.sender, delegatee);
68  }
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "decimals" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
65  function delegate(address delegatee) external {
66  return _delegate(msg.sender, delegatee);
67  }
68
69  /**
70  * @notice Delegates votes from signatory to `delegatee`
71  * @param delegatee The address to delegate votes to
72  * @param nonce The contract state required to match the signature
73  * @param expiry The time at which to expire the signature
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "totalSupply" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
70  * @notice Delegates votes from signatory to `delegatee`
71  * @param delegatee The address to delegate votes to
72  * @param nonce The contract state required to match the signature
73  * @param expiry The time at which to expire the signature
74  * @param v The recovery byte of the signature
75  * @param r Half of the ECDSA signature pair
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "transfer" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
86  external
87  {
88  bytes32 domainSeparator = keccak256(
89  abi.encode(
90  DOMAIN_TYPEHASH,
91  keccak256(bytes(name())),
92  getChainId(),
93  address(this)
94  )
95  );
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "allowance" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
95  );
96
97  bytes32 structHash = keccak256(
98  abi.encode(
99  DELEGATION_TYPEHASH,
100 delegatee,
101 nonce,
102 expiry
103 )
104 );
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "approve" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
107 abi.encodePacked(
108 "\x19\x01",
109 domainSeparator,
110 structHash
111 )
112 );
113
114 address signatory = ecrecover(digest, v, r, s);
115 require(signatory != address(0), "Kangaroo::delegateBySig: invalid signature");
116 require(nonce == nonces[signatory]++, "Kangaroo::delegateBySig: invalid nonce");
117 require(now <= expiry, "Kangaroo::delegateBySig: signature expired");
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "transferFrom" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
122 * @notice Gets the current votes balance for `account`
123 * @param account The address to get votes balance
124 * @return The number of current votes for `account`
125 */
126 function getCurrentVotes(address account)
127 external
128 view
129 returns (uint256)
130 {
131 uint32 nCheckpoints = numCheckpoints[account];
132 return nCheckpoints > 0 ? checkpoints[account][nCheckpoints - 1].votes : 0;
133 }
134
135 /**
136 * @notice Determine the prior number of votes for an account as of a block number
137 * @dev Block number must be a finalized block or else this function will revert to prevent misinformation.
138 * @param account The address of the account to check
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "increaseAllowance" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
140 * @return The number of votes the account had as of the given block
141 */
142 function getPriorVotes(address account, uint blockNumber)
143 external
144 view
145 returns (uint256)
146 {
147 require(blockNumber < block.number, "Kangaroo::getPriorVotes: not yet determined");
148
149 uint32 nCheckpoints = numCheckpoints[account];
150 if (nCheckpoints == 0) {
151 return 0;
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "decreaseAllowance" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
164 uint32 lower = 0;
165 uint32 upper = nCheckpoints - 1;
166 while (upper > lower) {
167 uint32 center = upper - (upper - lower) / 2; // ceil, avoiding overflow
168 Checkpoint memory cp = checkpoints[account][center];
169 if (cp.fromBlock == blockNumber) {
170 return cp.votes;
171 } else if (cp.fromBlock < blockNumber) {
172 lower = center;
173 } else {
```

MEDIUM

## Function could be marked as external.

SWC-000

The function definition of "mint" is marked "public". However, it is never directly called by another function in the same contract or in any of its descendants. Consider to mark it as "external" instead.

Source file

KangarooToken.sol

Locations

```
175 }
176 }
177 return checkpoints[account][lower].votes;
178 }
179
180 function _delegate(address delegator, address delegatee)
181 internal
182 {
183 address currentDelegate = _delegates[delegator];
184 uint256 delegatorBalance = balanceOf(delegator); // balance of underlying Kangaroos (not scaled);
185 _delegates[delegator] = delegatee;
```