MythX

Analysis 15564413-2658-47a3-a655-f3e85e65449b MythX

Started	Wed May 26 2021 20:03:36 GMT+0000 (Coordinated Universal Time)
Finished	Wed May 26 2021 20:39:17 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Remythx
Main Source File	Timelock.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	6	1

ISSUES

MEDIUM Function could be marked as external.

SWC-000

The function definition of "setDelay" 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

SafeMath.sol

Locations

```
100 *
101 * - The divisor cannot be zero.
102 */
103 function div(uint256 a, uint256 b) internal pure returns (uint256) {
104 return div(a, b, "SafeMath: division by zero");
105 }
106
107 /**
108 * @dev Returns the integer division of two unsigned integers. Reverts with custom message on
109 * division by zero. The result is rounded towards zero.
110 *
111 * Counterpart to Solidity's `/` operator. Note: this function uses a
112 * `revert` opcode (which leaves remaining gas untouched) while Solidity
113 * uses an invalid opcode to revert (consuming all remaining gas).
114 *
```

MEDIUM

Function could be marked as external.

SWC-000

The function definition of "acceptAdmin" 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

SafeMath.sol

Locations

```
110 *
111 * Counterpart to Solidity's `/` operator. Note: this function uses a
112 * `revert` opcode (which leaves remaining gas untouched) while Solidity
113 * uses an invalid opcode to revert (consuming all remaining gas).
114 *
115 * Requirements:
116 *
117 * - The divisor cannot be zero.
118 */
119 function div(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
120 require(b > 0, errorMessage);
121 uint256 c = a / b;
```

MEDIUM

Function could be marked as external.

SWC-000

The function definition of "setPendingAdmin" 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

SafeMath.sol

Locations

```
117 * - The divisor cannot be zero.
118 */
119 function div(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
120 require(b > 0, errorMessage);
121 uint256 c = a / b;
122 // assert(a == b * c + a % b); // There is no case in which this doesn't hold
123
124 return c;
125 }
126
127 /**
128 * @dev Returns the remainder of dividing two unsigned integers. (unsigned integer modulo),
129 * Reverts when dividing by zero.
130 *
131 * Counterpart to Solidity's `%` operator. This function uses a `revert`
132 * opcode (which leaves remaining gas untouched) while Solidity uses an
133 * invalid opcode to revert (consuming all remaining gas).
134 *
```

MEDIUM

Function could be marked as external.

SWC-000

The function definition of "queueTransaction" 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

SafeMath.sol

Locations

```
130 *
131 * Counterpart to Solidity's `%` operator. This function uses a `revert`
132 * opcode (which leaves remaining gas untouched) while Solidity uses an
133 * invalid opcode to revert (consuming all remaining gas).
134 *
135 * Requirements:
136 *
137 * - The divisor cannot be zero.
138 */
139 function mod(uint256 a, uint256 b) internal pure returns (uint256) {
140 return mod(a, b, "SafeMath: modulo by zero");
141 }
142
143 /**
144 * @dev Returns the remainder of dividing two unsigned integers. (unsigned integer modulo),
145 * Reverts with custom message when dividing by zero.
146 *
147 * Counterpart to Solidity's `%` operator. This function uses a `revert`
148 * opcode (which leaves remaining gas untouched) while Solidity uses an
149 * invalid opcode to revert (consuming all remaining gas).
150 *
```