MythX

REPORT 60D7B000A876B70019CAD763

Created	Sat Jun 26 2021 22:53:52 GMT+0000 (Coordinated Universal Time)
Number of analyses	1
User	60d275a243f2c37dbc12dde1

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
db93066c-fd38-4bd5-aa78-9ee8bdd8ba73	LoserCoin.sol	19

Analysis db93066c-fd38-4bd5-aa78-9ee8bdd8ba73 MythX

Started	Sat Jun 26 2021 22:54:01 GMT+0000 (Coordinated Universal Time)
Finished	Sat Jun 26 2021 22:56:11 GMT+0000 (Coordinated Universal Time)
Mode	Quick
Client Tool	Mythx-Cli-0.6.22
Main Source File	LoserCoin.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	16	3

ISSUES

MEDIUM

SWC-000

Function could be marked as external.

The function definition of "name" 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
LoserCoin.sol
Locations

```
164 }
165
166 function name() public view returns (string memory) {
167 return _name;
168 }
169
```

MEDIUM

SWC-000

Function could be marked as external.

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
LoserCoin.sol
Locations

```
169
170
171 function symbol() public view returns (string memory) {
172 return _symbol;
173 }
174
```

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

LoserCoin.sol

Locations

```
174
175
176 function decimals() public view returns (uint8) {
177 return _decimals;
178 }
179
```

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

LoserCoin.sol

Locations

```
179
180
181 function totalSupply() public view override returns (uint256) {
182 return _totalSupply;
183 }
184
```

MEDIUM

Function could be marked as external.

SWC-000

The function definition of "balanceOf" 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

LoserCoin.sol

Locations

```
184
185
186 function balanceOf(address account) public view override returns (uint256) {
187 return _balances[account];
188 }
189
```

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

LoserCoin.sol

Locations

```
189
190
191 function transfer(address recipient, uint256 amount) public virtual override returns (bool) {
192 _transfer(_msgSender(), recipient, amount);
193 return true;
194 }
195
```

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

LoserCoin.sol

Locations

```
195
196
197 function allowance(address owner, address spender) public view virtual override returns (uint256) {
198 return _allowances[owner][spender];
199 }
200
```

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

LoserCoin.sol

Locations

```
200
201
202 function approve(address spender, uint256 amount) public virtual override returns (bool) {
203 _approve(_msgSender(), spender, amount);
204 return true;
205 }
206
```

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

LoserCoin.sol

Locations

```
206
207
208 function transferFrom(address sender, address recipient, uint256 amount) public virtual override returns (bool) {
209 _transfer(sender, recipient, amount);
210 _approve(sender, _msgSender(), _allowances[sender][_msgSender()].sub(amount, "ERC20: transfer amount exceeds allowance"));
211 return true;
212 }
213
```

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

LoserCoin.sol

Locations

```
213
214
215 function increaseAllowance(address spender, uint256 addedValue) public virtual returns (bool) {
216 _approve(_msgSender(), spender, _allowances[_msgSender()][spender].add(addedValue));
217 return true;
218 }
219
220 function decreaseAllowance(address spender, uint256 subtractedValue) public virtual returns (bool) {
```

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

LoserCoin.sol

Locations

```
218 }
219
220 function decreaseAllowance(address spender, uint256 subtractedValue) public virtual returns (bool) {
221 _approve(_msgSender(), spender, _allowances[_msgSender()][spender].sub(subtractedValue, "ERC20: decreased allowance below zero"));
222 return true;
223 }
224
225 function _transfer(address sender, address recipient, uint256 amount) internal virtual {
```

MEDIUM

Function could be marked as external.

SWC-000

The function definition of "pause" 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

LoserCoin.sol

Locations

```
302 }
303
304 function pause() public onlyPauser{
305 _pause();
306 }
307
308 function unpause() public onlyPauser{
```

MEDIUM

Function could be marked as external.

SWC-000

The function definition of "unpause" 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

LoserCoin.sol

Locations

```
306 }
307
308 function unpause() public onlyPauser{
309 _unpause();
310 }
311
312 function changeUser(address new_operator, address new_pauser) public onlyFactory{
```

MEDIUM

Function could be marked as external.

SWC-000

The function definition of "changeUser" 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

LoserCoin.sol

Locations

```
310 }
311
312 function changeUser(address new_operator, address new_pauser) public onlyFactory{
313 _pauser=new_pauser;
314 _operator=new_operator;
315 }
316
317 function mint(address account, uint256 amount) public whenNotPaused onlyOperator {
```

MEDIUM

SWC-000

Function could be marked as external.

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

LoserCoin.sol

Locations

```
315 }
316
317 function mint(address account, uint256 amount) public whenNotPaused onlyOperator {
318 _mint(account, amount);
319 }
320 function burn(address account , uint256 amount) public whenNotPaused onlyOperator {
321 _burn(account,amount);
```

MEDIUM

SWC-000

Function could be marked as external.

The function definition of "burn" 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

LoserCoin.sol

Locations

```
318 _mint(account, amount);
319 }
320 function burn(address account , uint256 amount) public whenNotPaused onlyOperator {
321 _burn(account,amount);
322 }
323 }
```

LOW

SWC-131

Unused function parameter "from".

The value of the function parameter "from" for the function "_beforeTokenTransfer" of contract "ERC20" does not seem to be used anywhere in "_beforeTokenTransfer".

Source file

LoserCoin.sol

Locations

```
268 }
269
270 function _beforeTokenTransfer(address from, address to, uint256 amount) internal virtual { }
271 }
272 abstract contract ERC20Pausable is ERC20, Pausable {
```

LOW

Unused function parameter "to".

The value of the function parameter "to" for the function "_beforeTokenTransfer" of contract "ERC20" does not seem to be used anywhere in "_beforeTokenTransfer".

SWC-131

Source file

LoserCoin.sol

Locations

```
268 }
269
270 function _beforeTokenTransfer(address from, address to, uint256 amount) internal virtual { }
271 }
272 abstract contract ERC20Pausable is ERC20, Pausable {
```

LOW

Unused function parameter "amount".

The value of the function parameter "amount" for the function "_beforeTokenTransfer" of contract "ERC20" does not seem to be used anywhere in "_beforeTokenTransfer".

SWC-131

Source file

LoserCoin.sol

Locations

```
268 }
269
270 function _beforeTokenTransfer(address from, address to, uint256 amount) internal virtual { }
271 }
272 abstract contract ERC20Pausable is ERC20, Pausable {
```