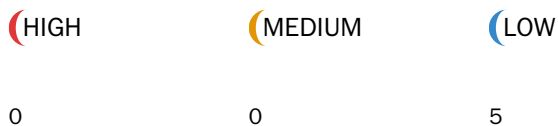


Started	Tue Mar 22 2022 15:52:43 GMT+0000 (Coordinated Universal Time)
Finished	Tue Mar 22 2022 16:38:26 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Mythx-Vscode-Extension
Main Source File	/Contracts/Royaltybearingtoken.Sol

DETECTED VULNERABILITIES



ISSUES

LOW

Use of "tx.origin" as a part of authorization control.

SWC-115

The tx.origin environment variable has been found to influence a control flow decision. Note that using "tx.origin" as a security control might cause a situation where a user inadvertently authorizes a smart contract to perform an action on their behalf. It is recommended to use "msg.sender" instead.

Source file

/contracts/royaltybearingtoken.sol

Locations

```

40  _setupRole(CREATOR_ROLE, creatorAddress); //v1.3
41
42  _numGenerations = numGenerations;
43
44  for (uint256 i = 0; i < allowedTokenTypes.length; i++) {

```

LOW

Use of "tx.origin" as a part of authorization control.

SWC-115

The tx.origin environment variable has been found to influence a control flow decision. Note that using "tx.origin" as a security control might cause a situation where a user inadvertently authorizes a smart contract to perform an action on their behalf. It is recommended to use "msg.sender" instead.

Source file

/contracts/royaltybearingtoken.sol

Locations

```

206
207  //royaltySplitForItsChildren must be less or equal to 100%
208  require(token.royaltySplitForItsChildren <= 10000, 'Royalty Split is > 100%');
209
210  //If the token cannot have offspring royaltySplitForItsChildren must be zero

```

LOW

Requirement violation.

A requirement was violated in a nested call and the call was reverted as a result. Make sure valid inputs are provided to the nested call (for instance, via passed arguments).

SWC-123

Source file

/contracts/royaltybearingtoken.sol

Locations

```
467 | uint256 tokenId,  
468 | bytes memory data  
469 | ) public override  
470 | //https://hackmd.io/0o70I-dRs5deopReWqTLbnw/r1NDumcBt#Payment-Parameter-Validation  
471 | (  
472 | address _seller,
```

LOW

Requirement violation.

A requirement was violated in a nested call and the call was reverted as a result. Make sure valid inputs are provided to the nested call (for instance, via passed arguments).

SWC-123

Source file

/contracts/royaltybearingtoken.sol

Locations

```
70 | }  
71 |  
72 | //https://hackmd.io/0afreund14031969/r1NDumcBt#Approach  
73 | function updateMaxGenerations(uint256 newMaxNumber) public virtual returns (bool) {  
74 | //ensure that msg.sender has the creator role or internal call  
75 | require(hasRole(CREATOR_ROLE, _msgSender()) || address(this) == _msgSender(), 'Creator role required');
```

Source file

/contracts/royaltybearingtoken.sol

Locations

```
70 | }  
71 |  
72 | //https://hackmd.io/0afreund14031969/r1NDumcBt#Approach  
73 | function updateMaxGenerations(uint256 newMaxNumber) public virtual returns (bool) {  
74 | //ensure that msg.sender has the creator role or internal call  
75 | require(hasRole(CREATOR_ROLE, _msgSender()) || address(this) == _msgSender(), 'Creator role required');
```

LOW

Requirement violation.

A requirement was violated in a nested call and the call was reverted as a result. Make sure valid inputs are provided to the nested call (for instance, via passed arguments).

SWC-123

Source file

/contracts/royaltybearingtoken.sol

Locations

```
563 | paymentModule.addRegisterPayment(_msgSender(), tokenIds, msg.value, 'ETH');
564 | } else if (trxnType == 0) {
565 | //encode payment data for transfer(s)
566 | bytes memory data = abi.encode(seller, _msgSender(), receiver, tokenIds, 'ETH', msg.value, address(this), block.chainid);
567 |
568 | //transfer NFT(s)
```