MythX

Analysis 4b0ca536-144c-4f98-b0ba-e368dea08bc6 MythX

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

HIGH	MEDIUM	LOW
0	0	5

ISSUES

LOW

SWC-115

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

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

```
_setupRole(CREATOR_ROLE, creatorAddress); //v1.3

_numGenerations = numGenerations;

for (uint256 i = 0; i < allowedTokenTypes.length; i++) {
```

LOW

SWC-115

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

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

```

//royaltySplitForItsChildren must be less or equal to 100%
require(token.royaltySplitForItsChildren <= 10000, 'Royalty Split is > 100%');

//If the token cannot have offspring royaltySplitForItsChildren must be zero
```

LOW

SWC-123

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).

Source file

/contracts/royaltybearingtoken.sol

Locations

```
uint256 tokenId,
bytes memory data
) public override {
//https://hackmd.io/@o70I-dRsSdeopRewqTLbnw/r1NDumcBt#Payment-Parameter-Validation
(
address _seller,
```

LOW

SWC-123

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).

Source file

/contracts/royaltybearingtoken.sol

Locations

```
}

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

Source file

/contracts/royaltybearingtoken.sol

Locations

```
}

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

LOW

SWC-123

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).

Source file

`/contracts/royaltybearingtoken.sol`

Locations

```
paymentModule.addRegisterPayment(_msgSender(), tokenIds, msg.value, 'ETH');
} else if (trxntype == 0) {
//encode payment data for transfer(s)
bytes memory data = abi.encode(seller, _msgSender(), receiver, tokenIds, 'ETH', msg.value, address(this), block.chainid);

//transfer NFT(s)
```