

REPORT 63733DF59FD866001A87C64E

Created	Tue Nov 15 2022 07:21:25 GMT+0000 (Coordinated Universal Time)
Number of analyses	1
User	63733ae2a86727333d355dc3

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
391d6e69-a963-49bf-87d4-e71c7eb68d55	BAPC.sol	4

Started	Tue Nov 15 2022 07:21:28 GMT+0000 (Coordinated Universal Time)
Finished	Tue Nov 15 2022 08:08:10 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Remythx
Main Source File	BAPC.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	4

ISSUES

LOW

A floating pragma is set.

SWC-103

The current pragma Solidity directive is ""^0.8.4"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

erc721a/IERC721A.sol

Locations

```
24 | error BalanceQueryForZeroAddress();
25 |
26 | /**
27 |  * Cannot mint to the zero address.
28 |  */
29 | error MintToZeroAddress();
```

LOW

Write to persistent state following external call.

SWC-107

The contract account state is accessed after an external call. To prevent reentrancy issues, consider accessing the state only before the call, especially if the callee is untrusted. Alternatively, a reentrancy lock can be used to prevent untrusted callees from re-entering the contract in an intermediate state.

Source file

@openzeppelin/contracts/security/ReentrancyGuard.sol

Locations

```
65 | // By storing the original value once again, a refund is triggered (see
66 | // https://eips.ethereum.org/EIPS/eip-2200)
67 | _status = _NOT_ENTERED;
68 | }
69 | }
```

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

erc721a/IERC721A.sol

Locations

```
71 |
72 | /**
73 |  * The `extraData` cannot be set on an unintia
74 |  */
75 | error OwnershipNotInitializedForExtraData();
```

LOW

Requirement violation.

SWC-123

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

erc721a/IERC721A.sol

Locations

```
150 |
151 | /**
152 |  * @dev Safely transfers `tokenId` token from `from` to `to`,
153 |  * checking first that contract recipients are aware of the ERC721 protocol
154 |  * to prevent tokens from being forever locked.
```