



[www.EtherAuthority.io](http://www.EtherAuthority.io)  
[audit@etherauthority.io](mailto:audit@etherauthority.io)

# SMART CONTRACT

---

## Security Audit Report

Project: NFTAuction  
Platform: Polygon Network  
Language: Solidity  
Date: April 9th, 2022

# Table of contents

Introduction .....	4
Project Background .....	4
Audit Scope .....	4
Claimed Smart Contract Features .....	5
Audit Summary .....	6
Technical Quick Stats .....	7
Code Quality .....	8
Documentation .....	8
Use of Dependencies .....	8
AS-IS overview .....	9
Severity Definitions .....	11
Audit Findings .....	12
Conclusion .....	14
Our Methodology .....	15
Disclaimers .....	17
Appendix	
• Code Flow Diagram .....	18
• Slither Results Log .....	19
• Solidity static analysis .....	21
• Solhint Linter .....	24

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

## Introduction

EtherAuthority was contracted by the NFTAuction team to perform the Security audit of the NFTAuction smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on April 9th, 2022.

**The purpose of this audit was to address the following:**

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

## Project Background

NFTAuction Contract is an NFT smart contract, having functions like getRoyalty, createAuction, createSale, makeBid, \_updateOngoingAuction, etc. The NFTAuction NFT contract inherits IERC721, IERC721Receiver, IERC20, IAccessControl, IERC2981, Ownable standard smart contracts from the OpenZeppelin library. These OpenZeppelin contracts are considered community- audited and time-tested, and hence are not part of the audit scope.

## Audit scope

<b>Name</b>	<b>Code Review and Security Analysis Report for NFTAuction Smart Contract</b>
<b>Platform</b>	<b>Polygon / Solidity</b>
<b>File</b>	NFTAuction.sol
<b>File MD5 Hash</b>	B2D6EFD5582C9267152D0F049016BC4B
<b>Audit Date</b>	April 9th, 2022

## Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
<p><b>Tokenomics:</b></p> <ul style="list-style-type: none"><li>• This contract can support the ERC2981 royalty standard.</li></ul>	<p><b>YES, This is valid.</b></p>
<p><b>Ownership control:</b></p> <ul style="list-style-type: none"><li>• Owner can set a bid increase percentage.</li><li>• Owner can set the maximum and minimum price percentage.</li><li>• Owner can set allowed ERC20 tokens.</li><li>• Owner can set max and min auction duration.</li><li>• Owner can auction the bid period.</li><li>• Owner can set the fee recipient and fee percentage.</li></ul>	<p><b>YES, This is valid.</b></p>

# Audit Summary

According to the standard audit assessment, Customer's solidity smart contracts are **"secure"**. This token contract does contain owner control, which does not make it fully decentralized.



We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.

All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

**We found 0 critical, 0 high, 0 medium and 0 low and some very low level issues.**

**Investors Advice:** Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

## Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Moderated
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Passed
Gas Optimization	"Out of Gas" Issue	Passed
	High consumption 'for/while' loop	Passed
	High consumption 'storage' storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	"Short Address" Attack	Passed
	"Double Spend" Attack	Passed

Overall Audit Result: **PASSED**

## Code Quality

This audit scope has 1 smart contract file. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in the NFTAuction contract are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the NFTAuction.

The NFTAuction team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are **not well** commented on smart contracts. Ethereum's NatSpec style for commenting is used, which is a good thing.

## Documentation

We were given a NFTAuction smart contract code in the form of File. The hash of that code is mentioned above in the table.

As mentioned above, code parts are **not well** commented. So it is not easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

## Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects.

Apart from libraries, its functions are used in external smart contract calls.



# AS-IS overview

## Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	onlyOwner	modifier	Passed	No Issue
3	owner	read	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	transferOwnership	internal	Passed	No Issue
7	auctionOngoing	modifier	Passed	No Issue
8	priceGreaterThanZero	modifier	Passed	No Issue
9	erc20TokensIsAllowed	modifier	Passed	No Issue
10	contractIsApproved	modifier	Passed	No Issue
11	minPriceDoesNotExceedLimit	modifier	Error message should be corrected	Refer Audit Finding
12	notNftSeller	modifier	Passed	No Issue
13	onlyNftSeller	modifier	Passed	No Issue
14	bidAmountMeetsBidRequirements	modifier	Passed	No Issue
15	onlyApplicableBuyer	modifier	Passed	No Issue
16	minimumBidNotMade	modifier	Passed	No Issue
17	paymentAccepted	modifier	Passed	No Issue
18	isAuctionOver	modifier	Passed	No Issue
19	auctionEndInsideOfBounds	modifier	Passed	No Issue
20	isAuctionOngoing	internal	Passed	No Issue
21	isABidMade	internal	Passed	No Issue
22	isMinimumBidMade	internal	Passed	No Issue
23	isBuyNowPriceMet	internal	Passed	No Issue
24	doesBidMeetBidRequirements	internal	Passed	No Issue
25	isWhitelistedSale	internal	Passed	No Issue
26	isAddressWhitelisted	internal	Passed	No Issue
27	isPaymentAccepted	internal	Passed	No Issue
28	isERC20Auction	internal	Passed	No Issue
29	getPortionOfBid	internal	Passed	No Issue
30	getRoyalty	write	Passed	No Issue
31	transferNftToAuctionContract	internal	Passed	No Issue
32	createAuction	internal	Passed	No Issue
33	createAuction	external	Passed	No Issue
34	createSale	external	Passed	No Issue
35	makeBid	internal	Passed	No Issue
36	makeBid	external	Passed	No Issue
37	updateOngoingAuction	internal	Passed	No Issue
38	resetAuction	internal	Passed	No Issue

39	_resetBids	internal	Passed	No Issue
40	_updateHighestBid	internal	Passed	No Issue
41	_reverseAndResetPreviousBid	internal	Passed	No Issue
42	_reversePreviousBidAndUpdateHighestBid	internal	Passed	No Issue
43	_transferNftAndPaySeller	internal	Passed	No Issue
44	_payFeesAndSeller	internal	Passed	No Issue
45	_payout	internal	Passed	No Issue
46	settleAuction	external	Passed	No Issue
47	withdrawAuction	external	Passed	No Issue
48	withdrawBid	external	Passed	No Issue
49	updateWhitelistedBuyers	external	Passed	No Issue
50	updateBuyNowPrice	external	Passed	No Issue
51	takeHighestBid	external	Passed	No Issue
52	withdrawAllFailedCredits	external	Passed	No Issue
53	setRoyalty	external	Passed	No Issue
54	setBidIncreasePercentage	external	access only Owner	No Issue
55	setMaximumMinPricePercentage	external	access only Owner	No Issue
56	setAuctionBidPeriod	external	access only Owner	No Issue
57	setFeeRecipient	external	access only Owner	No Issue
58	setErc20Token	external	access only Owner	No Issue
59	setAuctionDurationBounds	external	access only Owner	No Issue

## Severity Definitions

Risk Level	Description
<b>Critical</b>	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial
<b>Medium</b>	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
<b>Low</b>	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
<b>Lowest / Code Style / Best Practice</b>	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

# Audit Findings

## Critical Severity

No Critical severity vulnerabilities were found.

## High Severity

No High severity vulnerabilities were found.

## Medium

No Medium severity vulnerabilities were found.

## Low

No Low severity vulnerabilities were found.

## Very Low / Informational / Best practices:

(1) Error message should be corrected:

In the `minPriceDoesNotExceedLimit` modifier, the error message written is "MinPrice > 80% of buyNowPrice". But the % value can be changeable by the owner, so the error message should consider the value of the `maximumMinPricePercentage` variable for the % value.

```
modifier minPriceDoesNotExceedLimit(
    uint128 _buyNowPrice,
    uint128 _minPrice
) {
    require(
        _buyNowPrice == 0 ||
        getPortionOfBid(_buyNowPrice, maximumMinPricePercentage) >=
        _minPrice,
        "MinPrice > 80% of buyNowPrice" ←
    );
    _;
}
```

**Resolution:** We suggest changing the error message by replacing 80% with the parameter value set for `maximumMinPricePercentage`.

# Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble.

Following are Admin functions:

- `setBidIncreasePercentage`: The Owner can set bid increase Percentage value.
- `setMaximumMinPricePercentage`: The Owner can set the bid maximum and minimum price Percentage value.
- `setAuctionBidPeriod`: The Owner can set the auction bid period.
- `setFeeRecipient`: The Owner can set fee recipient
- `setErc20Token`: The Owner can set ERC20 Token value.
- `setAuctionDurationBounds`: The Owner can set auction duration bonds value.

## Conclusion

We were given a contract code. And we have used all possible tests based on given objects as files. We have not observed any major issue. So, **it's good to go for the mainnet deployment.**

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract, based on standard audit procedure scope, is **“Secured”**.

# Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

## **Manual Code Review:**

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

## **Vulnerability Analysis:**

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

## **Documenting Results:**

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

## **Suggested Solutions:**

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.



# Disclaimers

## EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

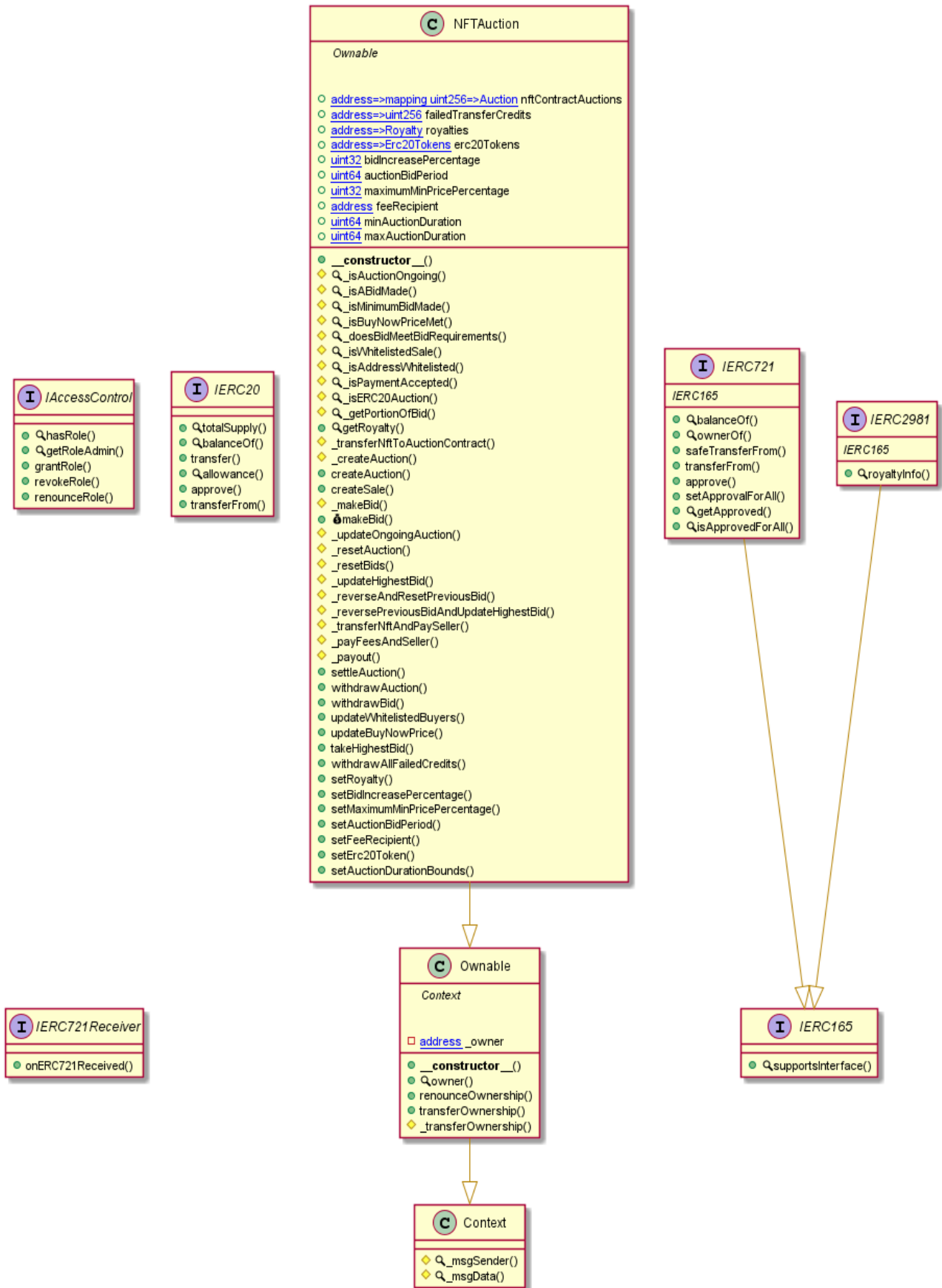
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

## Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can't guarantee explicit security of the audited smart contracts.

# Appendix

## Code Flow Diagram - NFTAuction



# Slither Results Log

## Slither log >> NFTAuction.sol

```
INFO:Detectors:
NFTAuction.constructor(address,uint32,uint32,uint64,uint64,uint64)._feeRecipient (NFTAuction.sol#672) lacks a zero-check on
- feeRecipient = _feeRecipient (NFTAuction.sol#682)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Reentrancy in NFTAuction._payout(address,uint256,address,uint256) (NFTAuction.sol#1340-1364):
  External calls:
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  State variables written after the call(s):
  - failedTransferCredits[_recipient] = failedTransferCredits[_recipient] + _amount (NFTAuction.sol#1359-1361)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2
INFO:Detectors:
Reentrancy in NFTAuction._createAuction(address,uint256,address,uint128,uint128,address[],uint256) (NFTAuction.sol#902-944)
  External calls:
  - _reverseAndResetPreviousBid(_nftContractAddress,_tokenId) (NFTAuction.sol#919)
  - IERC20(auctionERC20Token).transfer(_recipient,_amount) (NFTAuction.sol#1350)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  External calls sending eth:
  - _reverseAndResetPreviousBid(_nftContractAddress,_tokenId) (NFTAuction.sol#919)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  Event emitted after the call(s):
  - AuctionCreated(_nftContractAddress,_tokenId,msg.sender,_erc20Token,_minPrice,_buyNowPrice,_auctionEnd,_whiteliste
  uyers) (NFTAuction.sol#934-943)
Reentrancy in NFTAuction._makeBid(address,uint256,address,uint128) (NFTAuction.sol#1020-1054):
  External calls:
  - _reversePreviousBidAndUpdateHighestBid(_nftContractAddress,_tokenId,_tokenAmount) (NFTAuction.sol#1040-1044)
  - IERC20(auctionERC20Token).transferFrom(msg.sender,address(this),_tokenAmount) (NFTAuction.sol#1166-1170)
  - IERC20(auctionERC20Token).transfer(_recipient,_amount) (NFTAuction.sol#1350)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  External calls sending eth:
  - _reversePreviousBidAndUpdateHighestBid(_nftContractAddress,_tokenId,_tokenAmount) (NFTAuction.sol#1040-1044)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  Event emitted after the call(s):
  - BidMade(_nftContractAddress,_tokenId,msg.sender,msg.value,_erc20Token,_tokenAmount) (NFTAuction.sol#1045-1052)
Reentrancy in NFTAuction._makeBid(address,uint256,address,uint128) (NFTAuction.sol#1020-1054):
  External calls:
  - _reversePreviousBidAndUpdateHighestBid(_nftContractAddress,_tokenId,_tokenAmount) (NFTAuction.sol#1040-1044)

70)
  External calls sending eth:
  - _reversePreviousBidAndUpdateHighestBid(_nftContractAddress,_tokenId,_tokenAmount) (NFTAuction.sol#1040-1044)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  - _updateOngoingAuction(_nftContractAddress,_tokenId) (NFTAuction.sol#1053)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  Event emitted after the call(s):
  - NFTTransferredAndSellerPaid(_nftContractAddress,_tokenId,_nftSeller,_nftHighestBid,_nftHighestBidder,_erc20Token)
  (NFTAuction.sol#1273-1280)
  - _updateOngoingAuction(_nftContractAddress,_tokenId) (NFTAuction.sol#1053)
Reentrancy in NFTAuction._transferNftAndPaySeller(address,uint256) (NFTAuction.sol#1237-1281):
  External calls:
  - _payFeesAndSeller(_nftContractAddress,_tokenId,_nftSeller,_nftHighestBid) (NFTAuction.sol#1259-1264)
  - IERC20(auctionERC20Token).transfer(_recipient,_amount) (NFTAuction.sol#1350)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  - IERC721(_nftContractAddress).transferFrom(address(this),_nftHighestBidder,_tokenId) (NFTAuction.sol#1266-1270)
  External calls sending eth:
  - _payFeesAndSeller(_nftContractAddress,_tokenId,_nftSeller,_nftHighestBid) (NFTAuction.sol#1259-1264)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  Event emitted after the call(s):
  - NFTTransferredAndSellerPaid(_nftContractAddress,_tokenId,_nftSeller,_nftHighestBid,_nftHighestBidder,_erc20Token)
  (NFTAuction.sol#1273-1280)
Reentrancy in NFTAuction._updateOngoingAuction(address,uint256) (NFTAuction.sol#1085-1098):
  External calls:
  - _transferNftToAuctionContract(_nftContractAddress,_tokenId) (NFTAuction.sol#1090)
  - IERC721(_nftContractAddress).transferFrom(_nftSeller,address(this),_tokenId) (NFTAuction.sol#874-878)
  - _transferNftAndPaySeller(_nftContractAddress,_tokenId) (NFTAuction.sol#1091)
  - IERC20(auctionERC20Token).transfer(_recipient,_amount) (NFTAuction.sol#1350)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  - IERC721(_nftContractAddress).transferFrom(address(this),_nftHighestBidder,_tokenId) (NFTAuction.sol#1266-
  70)
  External calls sending eth:
  - _transferNftAndPaySeller(_nftContractAddress,_tokenId) (NFTAuction.sol#1091)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  Event emitted after the call(s):
  - NFTTransferredAndSellerPaid(_nftContractAddress,_tokenId,_nftSeller,_nftHighestBid,_nftHighestBidder,_erc20Token)
  (NFTAuction.sol#1273-1280)
  - IERC721(_nftContractAddress).transferFrom(_nftSeller,address(this),_tokenId) (NFTAuction.sol#874-878)
  - _transferNftAndPaySeller(_nftContractAddress,_tokenId) (NFTAuction.sol#1502)
  - IERC20(auctionERC20Token).transfer(_recipient,_amount) (NFTAuction.sol#1350)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  - IERC721(_nftContractAddress).transferFrom(address(this),_nftHighestBidder,_tokenId) (NFTAuction.sol#1266-
  70)
  External calls sending eth:
  - _transferNftAndPaySeller(_nftContractAddress,_tokenId) (NFTAuction.sol#1502)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  Event emitted after the call(s):
  - HighestBidTaken(_nftContractAddress,_tokenId) (NFTAuction.sol#1503)
  - NFTTransferredAndSellerPaid(_nftContractAddress,_tokenId,_nftSeller,_nftHighestBid,_nftHighestBidder,_erc20Token)
  (NFTAuction.sol#1273-1280)
  - _transferNftAndPaySeller(_nftContractAddress,_tokenId) (NFTAuction.sol#1502)
Reentrancy in NFTAuction.updateBuyNowPrice(address,uint256,uint128) (NFTAuction.sol#1466-1488):
  External calls:
  - _transferNftToAuctionContract(_nftContractAddress,_tokenId) (NFTAuction.sol#1485)
  - IERC721(_nftContractAddress).transferFrom(_nftSeller,address(this),_tokenId) (NFTAuction.sol#874-878)
  - _transferNftAndPaySeller(_nftContractAddress,_tokenId) (NFTAuction.sol#1486)
  - IERC20(auctionERC20Token).transfer(_recipient,_amount) (NFTAuction.sol#1350)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  - IERC721(_nftContractAddress).transferFrom(address(this),_nftHighestBidder,_tokenId) (NFTAuction.sol#1266-
  70)
  External calls sending eth:
  - _transferNftAndPaySeller(_nftContractAddress,_tokenId) (NFTAuction.sol#1486)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  Event emitted after the call(s):
  - NFTTransferredAndSellerPaid(_nftContractAddress,_tokenId,_nftSeller,_nftHighestBid,_nftHighestBidder,_erc20Token)
  (NFTAuction.sol#1273-1280)
  - _transferNftAndPaySeller(_nftContractAddress,_tokenId) (NFTAuction.sol#1486)
Reentrancy in NFTAuction.updateWhitelistedBuyers(address,uint256,address[]) (NFTAuction.sol#1430-1464):
  External calls:
  - _payout(_nftContractAddress,_tokenId,nftHighestBidder,nftHighestBid) (NFTAuction.sol#1451-1456)
  - IERC20(auctionERC20Token).transfer(_recipient,_amount) (NFTAuction.sol#1350)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
  External calls sending eth:
  - _payout(_nftContractAddress,_tokenId,nftHighestBidder,nftHighestBid) (NFTAuction.sol#1451-1456)
```

This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

Email: [audit@EtherAuthority.io](mailto:audit@EtherAuthority.io)

```
External calls:
- _reverseAndResetPreviousBid(_nftContractAddress,_tokenId) (NFTAuction.sol#1394)
  - IERC20(auctionERC20Token).transfer(_recipient,_amount) (NFTAuction.sol#1350)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
External calls sending eth:
- _reverseAndResetPreviousBid(_nftContractAddress,_tokenId) (NFTAuction.sol#1394)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
Event emitted after the call(s):
- AuctionWithdrawn(_nftContractAddress,_tokenId,msg.sender) (NFTAuction.sol#1398)
Reentrancy in NFTAuction.withdrawBid(address,uint256) (NFTAuction.sol#1401-1418):
External calls:
- _payout(_nftContractAddress,_tokenId,nftHighestBidder,nftHighestBid) (NFTAuction.sol#1415)
  - IERC20(auctionERC20Token).transfer(_recipient,_amount) (NFTAuction.sol#1350)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
External calls sending eth:
- _payout(_nftContractAddress,_tokenId,nftHighestBidder,nftHighestBid) (NFTAuction.sol#1415)
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
Event emitted after the call(s):
- BidWithdrawn(_nftContractAddress,_tokenId,msg.sender) (NFTAuction.sol#1417)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
NFTAuction._isAuctionOngoing(address,uint256) (NFTAuction.sol#690-700) uses timestamp for comparisons
Dangerous comparisons:
- (block.timestamp < auctionEndTimeStamp || (auctionEndTimeStamp == 0 && seller != address(0))) (NFTAuction.sol#699)
NFTAuction._updateHighestBid(address,uint256,uint128) (NFTAuction.sol#1156-1184) uses timestamp for comparisons
Dangerous comparisons:
- block.timestamp + auctionBidPeriod > nftContractAuctions[_nftContractAddress][_tokenId].auctionEnd (NFTAuction.sol#1181)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Context._msgData() (NFTAuction.sol#10-12) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.8.0 (NFTAuction.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7
solc-0.8.0 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
```

```
INFO:Detectors:
Low level call in NFTAuction._payout(address,uint256,address,uint256) (NFTAuction.sol#1340-1364):
  - (success) = address(_recipient).call{gas: 20000,value: _amount}() (NFTAuction.sol#1353-1356)
Low level call in NFTAuction.withdrawAllFailedCredits() (NFTAuction.sol#1509-1521):
  - (successfulWithdraw) = msg.sender.call{gas: 20000,value: amount}() (NFTAuction.sol#1516-1519)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Parameter NFTAuction.getRoyalty(address,uint256,uint256)._nftContractAddress (NFTAuction.sol#843) is not in mixedCase
Parameter NFTAuction.getRoyalty(address,uint256,uint256)._tokenId (NFTAuction.sol#843) is not in mixedCase
Parameter NFTAuction.getRoyalty(address,uint256,uint256)._price (NFTAuction.sol#843) is not in mixedCase
Parameter NFTAuction.createAuction(address,uint256,address,uint128,uint128,address[],uint256)._nftContractAddress (NFTAuction.sol#947) is not in mixedCase
Parameter NFTAuction.createAuction(address,uint256,address,uint128,uint128,address[],uint256)._tokenId (NFTAuction.sol#948) is not in mixedCase
Parameter NFTAuction.createAuction(address,uint256,address,uint128,uint128,address[],uint256)._erc20Token (NFTAuction.sol#949) is not in mixedCase
Parameter NFTAuction.createAuction(address,uint256,address,uint128,uint128,address[],uint256)._minPrice (NFTAuction.sol#950) is not in mixedCase
Parameter NFTAuction.createAuction(address,uint256,address,uint128,uint128,address[],uint256)._buyNowPrice (NFTAuction.sol#951) is not in mixedCase
Parameter NFTAuction.createAuction(address,uint256,address,uint128,uint128,address[],uint256)._whitelistedBuyers (NFTAuction.sol#952) is not in mixedCase
Parameter NFTAuction.createAuction(address,uint256,address,uint128,uint128,address[],uint256)._auctionEnd (NFTAuction.sol#953) is not in mixedCase
Parameter NFTAuction.createSale(address,uint256,address,uint128,address[])._nftContractAddress (NFTAuction.sol#983) is not in mixedCase
Parameter NFTAuction.createSale(address,uint256,address,uint128,address[])._tokenId (NFTAuction.sol#984) is not in mixedCase
Parameter NFTAuction.createSale(address,uint256,address,uint128,address[])._erc20Token (NFTAuction.sol#985) is not in mixedCase
Parameter NFTAuction.createSale(address,uint256,address,uint128,address[])._buyNowPrice (NFTAuction.sol#986) is not in mixedCase
Parameter NFTAuction.createSale(address,uint256,address,uint128,address[])._whitelistedBuyers (NFTAuction.sol#987) is not in mixedCase
Parameter NFTAuction.makeBid(address,uint256,address,uint128)._nftContractAddress (NFTAuction.sol#1057) is not in mixedCase
Parameter NFTAuction.makeBid(address,uint256,address,uint128)._tokenId (NFTAuction.sol#1058) is not in mixedCase
Parameter NFTAuction.makeBid(address,uint256,address,uint128)._erc20Token (NFTAuction.sol#1059) is not in mixedCase
Parameter NFTAuction.makeBid(address,uint256,address,uint128)._tokenAmount (NFTAuction.sol#1060) is not in mixedCase
```

```
Parameter NFTAuction.setErc20Token(address,bool,uint32)._feePercentage (NFTAuction.sol#1573) is not in mixedCase
Parameter NFTAuction.setAuctionDurationBounds(uint64,uint64)._minAuctionDuration (NFTAuction.sol#1579) is not in mixedCase
Parameter NFTAuction.setAuctionDurationBounds(uint64,uint64)._maxAuctionDuration (NFTAuction.sol#1579) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable NFTAuction.makeBid(address,uint256,address,uint128)._erc20Token (NFTAuction.sol#1059) is too similar to NFTAuction.erc20Tokens (NFTAuction.sol#425)
Variable NFTAuction._createAuction(address,uint256,address,uint128,uint128,address[],uint256)._erc20Token (NFTAuction.sol#949) is too similar to NFTAuction.erc20Tokens (NFTAuction.sol#425)
Variable NFTAuction.createSale(address,uint256,address,uint128,address[])._erc20Token (NFTAuction.sol#985) is too similar to NFTAuction.erc20Tokens (NFTAuction.sol#425)
Variable NFTAuction.createAuction(address,uint256,address,uint128,uint128,address[],uint256)._erc20Token (NFTAuction.sol#949) is too similar to NFTAuction.erc20Tokens (NFTAuction.sol#425)
Variable NFTAuction._transferNftAndPaySeller(address,uint256)._erc20Token (NFTAuction.sol#1253-1255) is too similar to NFTAuction.erc20Tokens (NFTAuction.sol#425)
Variable NFTAuction._makeBid(address,uint256,address,uint128)._erc20Token (NFTAuction.sol#1023) is too similar to NFTAuction.erc20Tokens (NFTAuction.sol#425)
Variable NFTAuction.setErc20Token(address,bool,uint32)._erc20Token (NFTAuction.sol#1573) is too similar to NFTAuction.erc20Tokens (NFTAuction.sol#425)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-too-similar
INFO:Detectors:
renounceOwnership() should be declared external:
  - Ownable.renounceOwnership() (NFTAuction.sol#49-51)
transferOwnership(address) should be declared external:
  - Ownable.transferOwnership(address) (NFTAuction.sol#57-60)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:NFTAuction.sol analyzed (9 contracts with 75 detectors), 84 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

Email: [audit@EtherAuthority.io](mailto:audit@EtherAuthority.io)

# Solidity Static Analysis

## NFTAuction.sol

### Security

#### Check-effects-interaction: ✕

Potential violation of Checks-Effects-Interaction pattern in NFTAuction.\_updateHighestBid(address,uint256,uint128): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.

[more](#)

Pos: 1230:23:

#### Check-effects-interaction: ✕

Potential violation of Checks-Effects-Interaction pattern in NFTAuction.\_transferNftAndPaySeller(address,uint256): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.

[more](#)

Pos: 1330:37:

#### Block timestamp: ✕

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.

[more](#)

Pos: 1255:20:

#### Block timestamp: ✕

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.

[more](#)

Pos: 1263:1:

#### Low level calls: ✕

Use of "call": should be avoided whenever possible. It can lead to unexpected behavior if return value is not handled properly. Please use Direct Calls via specifying the called contract's interface.

[more](#)

Pos: 1431:18:

#### Low level calls: ✕

Use of "call": should be avoided whenever possible. It can lead to unexpected behavior if return value is not handled properly. Please use Direct Calls via specifying the called contract's interface.

[more](#)

Pos: 1587:218:

## Gas & Economy

### Gas costs:

Gas requirement of function `NFTAuction.getRoyalty` is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 857:13:

### Gas costs:

Gas requirement of function `NFTAuction.setAuctionDurationBounds` is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 1587:3485:

### Delete dynamic array:

The "delete" operation when applied to a dynamically sized array in Solidity generates code to delete each of the elements contained. If the array is large, this operation can surpass the block gas limit and raise an OOG exception. Also nested dynamically sized objects can produce the same results.

[more](#)

Pos: 1182:112:

### For loop over dynamic array:

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point. Additionally, using unbounded loops incurs in a lot of avoidable gas costs. Carefully test how many items at maximum you can pass to such functions to make it successful.

[more](#)

Pos: 804:6:

## Miscellaneous

### Constant/View/Pure functions:

`IAccessControl.grantRole(bytes32,address)` : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.

[more](#)

Pos: 123:4:

### Similar variable names:

`NFTAuction.setAuctionDurationBounds(uint64,uint64)` : Variables have very similar names "`_minAuctionDuration`" and "`_maxAuctionDuration`". Note: Modifiers are currently not considered by this static analysis.

Pos: 1587:3828:

### Guard conditions:



Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

[more](#)

Pos: 908:17:

### Guard conditions:



Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

[more](#)

Pos: 1478:0:

### No return:



IERC721.isApprovedForAll(address,address): Defines a return type but never explicitly returns a value.

Pos: 385:4:

### No return:



IERC2981.royaltyInfo(uint256,uint256): Defines a return type but never explicitly returns a value.

Pos: 393:4:

### Guard conditions:



Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

[more](#)

Pos: 1587:1124:

### Guard conditions:



Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

[more](#)

Pos: 1587:1408:

### Data truncated:



Division of integer values yields an integer value again. That means e.g.  $10 / 100 = 0$  instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.

Pos: 850:27:

### Data truncated:



Division of integer values yields an integer value again. That means e.g.  $10 / 100 = 0$  instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.

Pos: 868:13:

# Solhint Linter

## NFTAuction.sol

```
NFTAuction.sol:2:1: Error: Compiler version ^0.8.0 does not satisfy the r semver requirement
NFTAuction.sol:23:5: Error: Explicitly mark visibility in function (Set ignoreConstructors to true if using solidity >=0.7.0)
NFTAuction.sol:660:17: Error: Avoid to make time-based decisions in your business logic
NFTAuction.sol:660:72: Error: Avoid to make time-based decisions in your business logic
NFTAuction.sol:671:5: Error: Explicitly mark visibility in function (Set ignoreConstructors to true if using solidity >=0.7.0)
NFTAuction.sol:699:17: Error: Avoid to make time-based decisions in your business logic
NFTAuction.sol:1181:12: Error: Avoid to make time-based decisions in your business logic
NFTAuction.sol:1182:77: Error: Avoid to make time-based decisions in your business logic
NFTAuction.sol:1353:32: Error: Avoid using low level calls.
NFTAuction.sol:1359:17: Error: Possible reentrancy vulnerabilities. Avoid state changes after transfer.
NFTAuction.sol:1516:39: Error: Avoid using low level calls.
```

### Software analysis result:

These software reported many false positive results and some are informational issues.

So, those issues can be safely ignored.





This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

**Email: [audit@EtherAuthority.io](mailto:audit@EtherAuthority.io)**