SMART CONTRACT AUDIT

P R O J E C T :

U N I C O R N . W I N

METHODOLOGY

Main tests list:

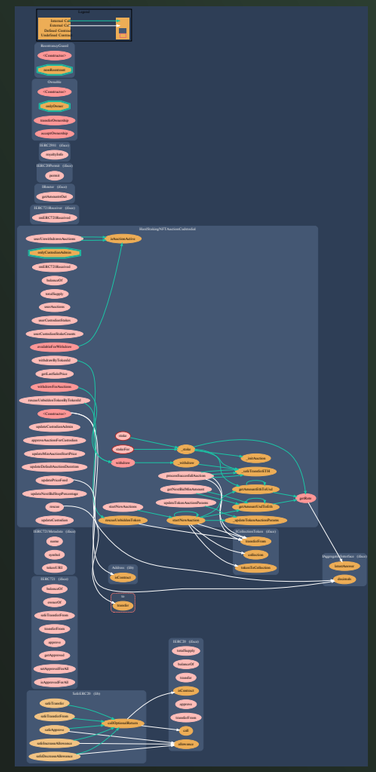
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unsed vars
- Uncheked call return method
- Code with no effects
- Function visibility
- Use of deprecated functions
- Authorization issues
- Re-entrancy
- Arithmetic Over/Under Flows
- Hidden Malicious Code
- External Contract Referencing
- Short Address/ Parameter Attack
- Race Conditions / Front Running
- Uninitialized Storage Pointers
- Floating Points and Precision
- Signatures Replay
- Pool Asset Security (backdoors in the underlying ERC-20)

STRUCTURE OF CONTRACT
HARDSTAKINGNFTAUCTIONCUDSTODIAL.SOL

Contract methods analysis

function onERC721Received(address operator, address from, uint256 tokenId, bytes calldata data) external pure override returns (bytes4)
Vulnerabilities not detected

function balanceOf(address account) external view returns (uint)
Vulnerabilities not detected



Pic. 1.1.
HardStakingNFTAuctionCudstodial.sol

function totalSupply() external view returns (uint)
Vulnerabilities not detected

unction userAuctions(address user) external view returns (uint[] memory auctionIds)
Vulnerabilities not detected

function userCustodianStakes(address user) external view returns (uint[] memory auctionIds)
Vulnerabilities not detected

function userCustodianStakeCounts(address user) external view returns (uint)
Vulnerabilities not detected

function userUnwithdrawnAuctions(address user) external view returns (uint[] memory auctionIds)
Vulnerabilities not detected

function availableForWithdraw(address user, uint auctionId) public view returns (uint actualStake)
Vulnerabilities not detected

function getNextBidMinAmount(uint auctionId) external view returns (uint actualBid, uint convertedBid)
Vulnerabilities not detected

function isAuctionActive(uint auctionId) public view returns (bool)
Vulnerabilities not detected

unction getRate() public view returns (uint)
Vulnerabilities not detected

function getAmountEthToUsd(uint amountEth) public view returns (uint)
Vulnerabilities not detected

function getAmountEthToUsd(uint amountEth, uint rate) public pure returns (uint)
Vulnerabilities not detected

function getAmountUsdToEth(uint amountUsd) public view returns (uint)
Vulnerabilities not detected

function getAmountUsdToEth(uint amountUsd, uint rate) public pure returns (uint)
Vulnerabilities not detected

function getLastSalePrice(uint tokenId) external view returns (uint)
Vulnerabilities not detected

function stake(uint auctionId)
Vulnerabilities not detected

function stakeFor(uint auctionId, address user)
Vulnerabilities not detected

function withdraw(uint auctionId)
Vulnerabilities not detected

function withdrawByTokenId(uint tokenId)
Vulnerabilities not detected

function withdrawForAuctions(uint[] memory auctionIds)
Vulnerabilities not detected

PAYABLE

function processSuccesfullAuction(uint auctionId)
In case you have added check for auction.auctionEnd != 0, winner can never be 0, so part of logic that handles it is redundant and can be removed. This method doesn't provide payable modifier from function, so in case royalty fee is required in FUN NFT it can not be processed.

FT out to winner, ETH out to NFT author(royalty fee) + owner(auction fee) + auction creator, can be called by anyone

function startNewAuctions(uint[] memory tokenIds, uint[] memory startBidAmounts, bool[] memory isAmountInEths, uint[] memory roundDurations, bool[] memory isCustodials, string[] memory descriptions)
Vulnerabilities not detected

function startNewAuction(uint tokenId, uint startBidAmount, bool isAmountInEth, uint roundDuration, uint successAuctionFeePercentage, string memory description, bool isCustodial)
Vulnerabilities not detected

PAYABLE

function startNewAuction(uint tokenId, uint startBidAmount, bool isAmountInEth, string memory description, bool isCustodial)
Vulnerabilities not detected

NFT in, can be called by anyone

function rescueUnbiddenTokenByTokenId(uint tokenId)
Vulnerabilities not detected

PAYABLE

function rescueUnbiddenToken(uint auctionId)
Vulnerabilities not detected

NFT out, can be called by auction owner

PAYABLE

function _stake(uint auctionId, address user)
Vulnerabilities not detected

ETH in, can be called by anyone

PAYABLE

function _withdraw(uint auctionId)
Vulnerabilities not detected

ETH out, can be called by anyone
rescue(address to, address tokenAddress, uint amount) - ERC20 out, can be called by owner

function _withdraw(uint auctionId)
Vulnerabilities not detected

function _initAuction(uint auctionId)
Vulnerabilities not detected

function _safeTransferETH(address to, uint value)
Vulnerabilities not detected

function updateCustodianAdmin(address newAdmin)
Vulnerabilities not detected

function approveAuctionForCustodian(uint auctionId, bool isApproved)
Vulnerabilities not detected

function updateMinAuctionStartPrice(uint newMinAuctionStartPrice)
Function should emit an event

function updateDefaultAuctionDuration(uint newDefaultAuctionDuration)
Function should emit an event

function updatePriceFeed(address newPriceFeed)
Vulnerabilities not detected

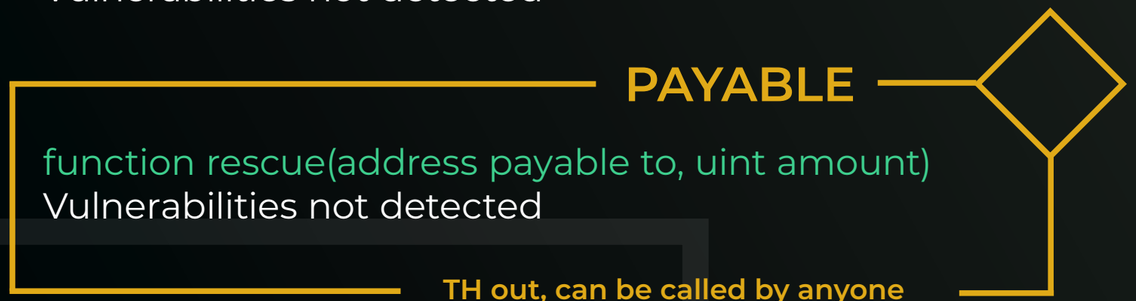
function updateTokenAuctionParams(uint tokenId, uint auctionRoundDuration, uint successAuctionFeePercentage)
Vulnerabilities not detected

function _updateTokenAuctionParams(uint tokenId, uint auctionRoundDuration, uint successAuctionFeePercentage)
Vulnerabilities not detected

function updateNextBidStepPercentage(uint newNextBidStepPercentage)
Vulnerabilities not detected

function rescue(address to, address tokenAddress, uint amount)
Vulnerabilities not detected

function updateCustodian(address newCustodian)
Vulnerabilities not detected



STRUCTURE OF CONTRACT
FUN.SOL

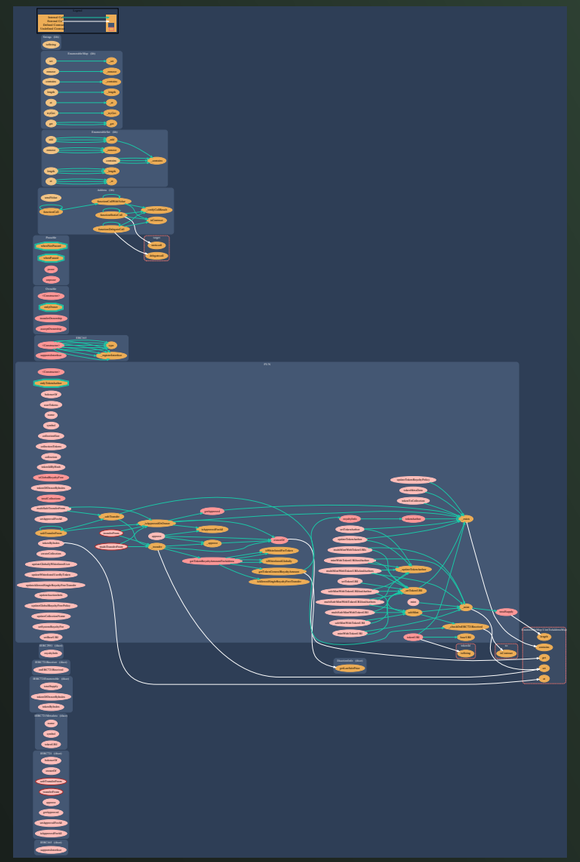
Typo in constructor: rayaltyFee

Contract methods analysis

function balanceOf(address owner) external view virtual override returns (uint)
Vulnerabilities not detected

function userTokens(address owner) external view virtual returns (uint[] memory)
Vulnerabilities not detected

function ownerOf(uint tokenId) public view virtual override returns (address)
Vulnerabilities not detected



Pic. 1.2.
FUN.sol

function name() external view virtual override returns (string memory)
Vulnerabilities not detected

function symbol() external view virtual override returns (string memory)
Vulnerabilities not detected

function tokenMetaData(uint tokenId) external view virtual returns (TokenMetaData memory)
Vulnerabilities not detected

function collectionSize(uint collectionId) external view virtual returns (uint)
Vulnerabilities not detected

function collectionTokens(uint collectionId) external view virtual returns (uint[] memory)
Vulnerabilities not detected

function collection(uint collectionId) external view virtual returns (Collection memory)
Vulnerabilities not detected

function tokenToCollection(uint tokenId) external view virtual returns (uint)
Vulnerabilities not detected

function tokenURI(uint tokenId) public view virtual override returns (string memory)
Function should be declared external

function tokenAuthor(uint tokenId) public view virtual returns (address)
Vulnerabilities not detected

function tokenIdByHash(string memory tokenHash) external view virtual returns (uint)
Vulnerabilities not detected

function royaltyInfo(uint _tokenId, uint _salePrice) public override view returns (address receiver, uint royaltyAmount)
Vulnerabilities not detected

function isWhitelistedGlobally(address user) public view virtual returns (bool)
Vulnerabilities not detected

function isWhitelistedForToken(address user, uint tokenId) public view virtual returns (bool)
Vulnerabilities not detected

function isAllowedSingleRoyaltyFreeTransfer(address from, address to, uint tokenId) public view virtual returns (bool)
Vulnerabilities not detected

function isGlobalRoyaltyFree() public view virtual returns (bool)
Function should be declared external

function getTokenRoyaltyAmountForAddress(address from, address to, uint tokenId) public view returns (address receiver, uint royaltyAmount)
Vulnerabilities not detected

function getTokenGeneralRoyaltyAmount(uint tokenId) public view returns (address receiver, uint royaltyAmount)
Vulnerabilities not detected

function baseURI() public view virtual returns (string memory)
Vulnerabilities not detected

function tokenOfOwnerByIndex(address owner, uint index) external view virtual override returns (uint)
Vulnerabilities not detected

function totalSupply() public view virtual override returns (uint)
Vulnerabilities not detected

function totalCollections() public view virtual returns (uint)
Function should be declared external

function tokenByIndex(uint index) external view virtual override returns (uint)
Vulnerabilities not detected

function approve(address to, uint tokenId)
Vulnerabilities not detected

function getApproved(uint tokenId) public view virtual override returns (address)
Vulnerabilities not detected

function setApprovalForAll(address operator, bool approved)
Vulnerabilities not detected

function isApprovedForAll(address owner, address operator) public view virtual override returns (bool)
Vulnerabilities not detected

function transferFrom(address from, address to, uint tokenId)
Vulnerabilities not detected

function multiTransferFrom(address[] memory from, address[] memory to, uint[] memory tokenId)
Vulnerabilities not detected

function safeTransferFrom(address from, address to, uint tokenId)
Vulnerabilities not detected

function safeTransferFrom(address from, address to, uint tokenId, bytes memory _data)
Vulnerabilities not detected

function multiSafeTransferFrom(address[] memory from, address[] memory to, uint[] memory tokenId, bytes[] memory _data)
Vulnerabilities not detected

function _safeTransfer(address from, address to, uint tokenId, bytes memory _data)
Vulnerabilities not detected

function _exists(uint tokenId) internal view virtual returns (bool)
Vulnerabilities not detected

function _isApprovedOrOwner(address spender, uint tokenId) internal view virtual returns (bool)
Vulnerabilities not detected

PAYABLE

function _transfer(address from, address to, uint tokenId)
Vulnerabilities not detected

ETH in, ETH out to author for royalty fee, NFT out, can be called by anyone

function _checkOnERC721Received(address from, address to, uint tokenId, bytes memory _data)
Vulnerabilities not detected

function _approve(address to, uint tokenId)
Vulnerabilities not detected

function createCollection(uint maxCollectionSize, bool isDigitalObject, string memory collectionName) external virtual onlyOwner returns (uint collectionId)
Vulnerabilities not detected

function updateGloballyWhitelistedUser(address user, bool isWhitelisted)
Vulnerabilities not detected

function updateWhitelistedUserByToken(address user, uint tokenId, bool isWhitelisted)
Vulnerabilities not detected

function updateAllowedSingleRoyaltyFreeTransfer(address from, address to, uint tokenId, bool isAllowed)
Vulnerabilities not detected

function updateAuctionInfo(address newAuctionInfo)
Vulnerabilities not detected

function updateGlobalRoyaltyFreePolicy(bool isGlobalRoyaltyFree)
Vulnerabilities not detected

function updateCollectionName(uint collectionId, string memory collectionName)
Vulnerabilities not detected

function mint(uint collectionId, address to) external virtual onlyOwner returns (uint tokenId)
Vulnerabilities not detected

function mintWithTokenURI(uint collectionId, address to, string memory tokenUri) external virtual onlyOwner returns (uint tokenId)
Vulnerabilities not detected

function mintWithTokenURIAndAuthor(uint collectionId, address to, string memory tokenUri, address author) external virtual onlyOwner returns (uint tokenId)
Vulnerabilities not detected

function safeMintWithTokenURI(uint collectionId, address to, string memory tokenUri, bytes memory _data) external virtual returns (uint tokenId)
Vulnerabilities not detected

function safeMintWithTokenURIAndAuthor(uint collectionId, address to, string memory tokenUri, address author, bytes memory _data) external virtual returns (uint tokenId)
Vulnerabilities not detected

function safeMint(uint collectionId, address to, bytes memory _data) public virtual onlyOwner returns (uint tokenId)
Vulnerabilities not detected

function multiSafeMintWithTokenURI(uint[] memory collectionIds, address[] memory to, string[] memory tokenURIs, bytes[] memory _data) external virtual returns (uint lastTokenId)
Vulnerabilities not detected

function multiSafeMintWithTokenURIAndAuthors(uint[] memory collectionIds, address[] memory to, string[] memory tokenURIs, address[] memory tokenAuthors, bytes[] memory _data) external virtual returns (uint lastTokenId)
Vulnerabilities not detected

function multiMintWithTokenURIs(uint[] memory collectionIds, address[] memory to, string[] memory tokenURIs) external virtual onlyOwner returns (uint lastTokenId)
Vulnerabilities not detected

function multiMintWithTokenURIsAndAuthors(uint[] memory collectionIds, address[] memory to, string[] memory tokenURIs, address[] memory tokenAuthors) external virtual onlyOwner returns (uint lastTokenId)
Vulnerabilities not detected

function setTokenURI(uint tokenId, string memory tokenUri)
Vulnerabilities not detected

function setSystemRoyaltyFee(uint newFee)
Vulnerabilities not detected

function setTokenAuthor(uint tokenId, address author)
Vulnerabilities not detected

function updateTokenAuthor(uint tokenId, address newAuthor) external virtual onlyTokenAuthor(tokenId)
Vulnerabilities not detected

function updateTokenRoyaltyPolicy(uint tokenId, bool isRoyaltyFree) external virtual onlyTokenAuthor(tokenId)
Vulnerabilities not detected

function setBaseURI(string memory baseURI_)
Vulnerabilities not detected

function _mint(uint collectionId, address to) internal virtual returns (uint tokenId)
Vulnerabilities not detected

function _setTokenURI(uint tokenId, string memory tokenUri, bool newToken)
Vulnerabilities not detected

function _updateTokenAuthor(uint tokenId, address previousAuthir, address newAuthor)
Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimization	Bytecode hash (SHA 256)
FUN	**0.8.7**	**200**	-1696a221f656097411d-009f945bdc-6cd55bb42d67dbc3834ba-0b5320ee222995
HardStakingNFTAuction-Cudstodial	**0.8.7**	**200**	e70060b786d2f-38579c5cadd2b97fed-48227f28b472872f-8f83624a18e65d30f

GET IN TOUCH

info@smartstate.tech
smartstate.tech