SMART CONTRACT AUDIT

NIFTSY

PROJECT:
NIFTSY

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
WRAPPERBASE.SOL

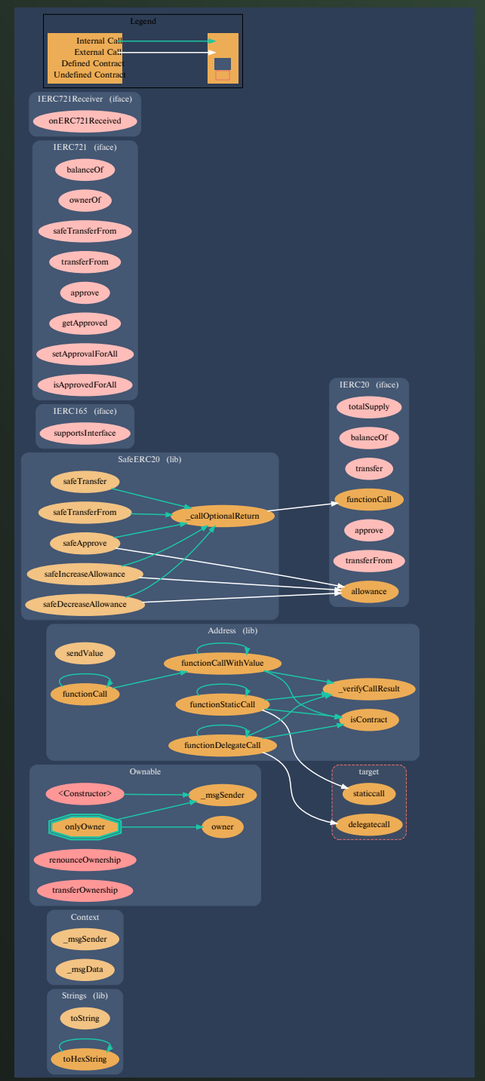
Vulnerabilities not detected

Contract methods analysis

wrap721(
address _underlineContract,
uint256 _tokenId,
uint256 _unwrapAfter,
uint256 _transferFee,
address _royaltyBeneficiary,
uint256 _royaltyPercent,
uint256 _unwraptFeeThreshold
)
Vulnerabilities not detected

addNativeCollateral(uint256 _wrappedTokenId)
Vulnerbilities not detected

unWrap721(uint256 _tokenId)
Vulnerabilities not detected



Pic. 1.1.
WrapperBase.sol

tokenURI(uint256 _tokenId)
Vulnerbilities not detected

getTokenValue(uint256 _tokenId)
Vulnerbilities not detected

getWrappedToken(uint256 _tokenId)
Vulnerbilities not detected

setFee(uint256 _fee, uint256 _startDate)
Vulnerbilities not detected

_beforeTokenTransfer(address from, address to, uint256 tokenId)
Vulnerabilities not detected

_chargeFee(address _payer, uint256 _amount)
Vulnerabilities not detected

_beforeUnWrapHook(uint256 _tokenId)
Vulnerabilities not detected

_getProtokolFeeAmount()
Vulnerabilities not detected

STRUCTURE OF CONTRACT
WRAPPERWITHERC20COLLATERAL.SOL

Constrcutor lacks check for 0 address.

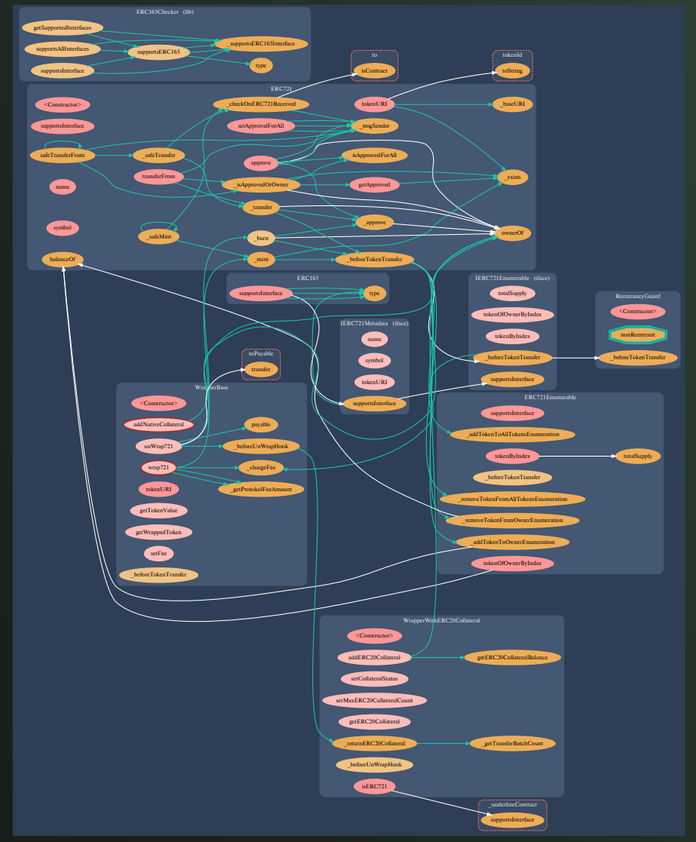
Contract methods analysis

addERC20Collateral(uint256 _wrappedTokenId, address _erc20, uint256 _amount)
Vulnerabilities not detected

setCollateralStatus(address _erc20, bool _isEnabled)
Vulnerabilities not detected

setMaxERC20CollateralCount(uint16 _count)
Vulnerabilities not detected

getERC20Collateral(uint256 _wrappedId)
Vulnerbilities not detected



Pic. 1.2.
WrapperBase.sol

getERC20CollateralBalance(uint256 _wrappedId, address _erc20)
Vulnerbilities not detected

isERC721(address _underlineContract, bytes4 _interfaceId)
Vulnerabilities not detected

_beforeUnWrapHook(uint256 _tokenId)
Vulnerabilities not detected

_returnERC20Collateral(uint256 _tokenId)
Vulnerabilities not detected

_getTransferBatchCount()
Vulnerbilities not detected

GET IN TOUCH

info@smartstate.tech
smartstate.tech