SMART CONTRACT AUDIT

BullPerks

PROJECT: BULLPERKS

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
BLPDEAL.SOL

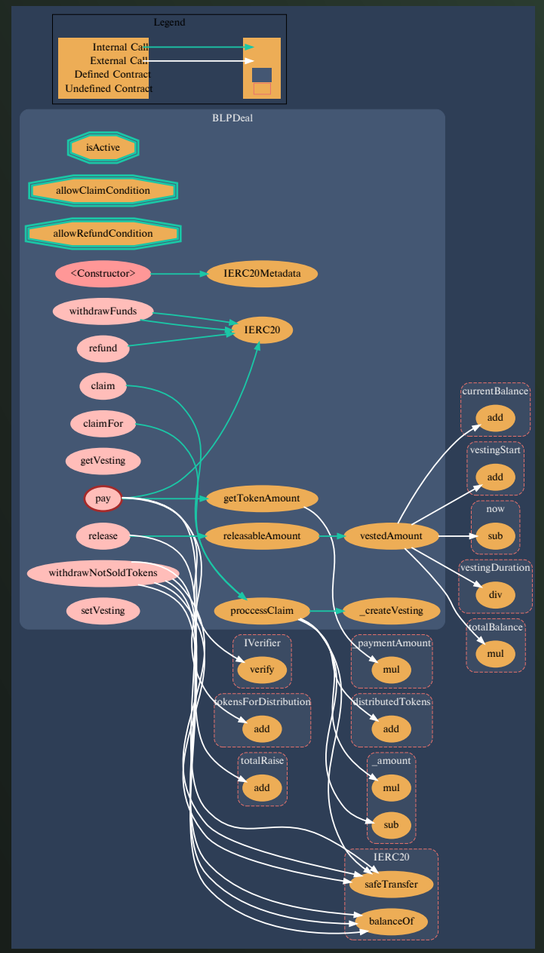
Contract methods analysis

pay(uint256 _amount, bytes memory _signature)
Vulnerabilities not detected

getTokenAmount(uint256 _paymentAmount)
Vulnerabilities not detected

claimFor(address[] memory _addresses)
Vulnerabilities not detected

claim()
Vulnerabilities not detected



Pic.1.1.
BLPDeal.sol

proccessClaim(address _receiver)
Vulnerabilities not detected

refund()
Vulnerabilities not detected

getVesting(address _beneficiary)
Vulnerabilities not detected

_createVesting(address _beneficiary, uint256 _amount)
Vulnerabilities not detected

release(address _beneficiary)
Vulnerabilities not detected

releasableAmount(address _beneficiary)
Vulnerabilities not detected

vestedAmount(address _beneficiary)
Vulnerabilities not detected

withdrawFunds()
Vulnerabilities not detected

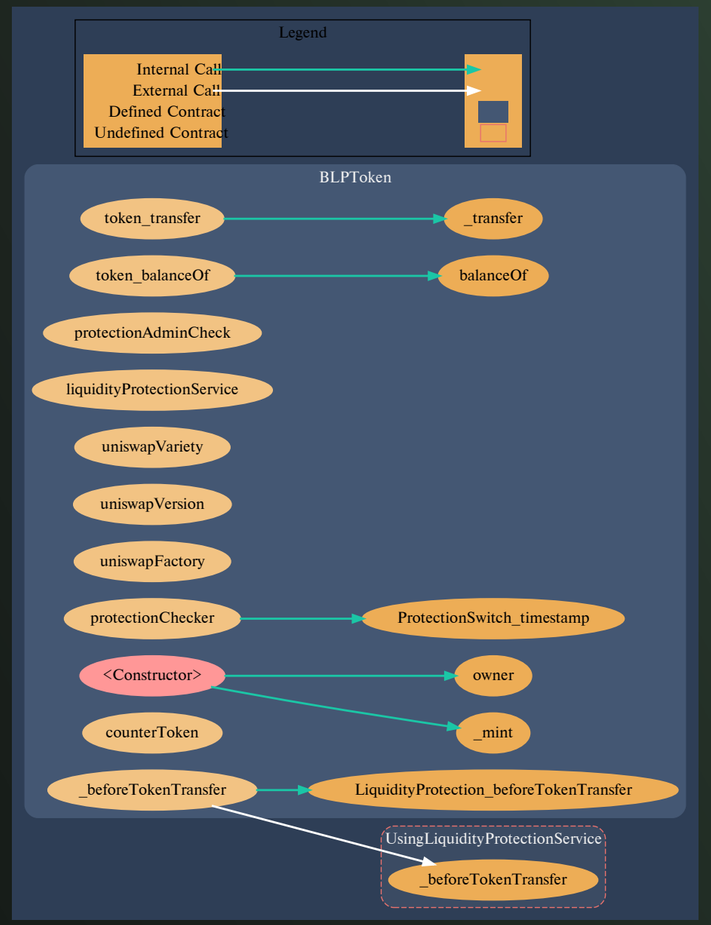
withdrawNotSoldTokens(bool _emergency)
Vulnerabilities not detected

setVesting(uint256 _percent,
uint256 _start,
uint256 _interval,
uint256 _duration)
Vulnerabilities not detected

STRUCTURE OF CONTRACT

BLPTOKEN.SOL

Vulnerabilities not detected



Pic.1.2.

BLPToken.sol

STRUCTURE OF CONTRACT

BLPTOKENVESTING.SOL

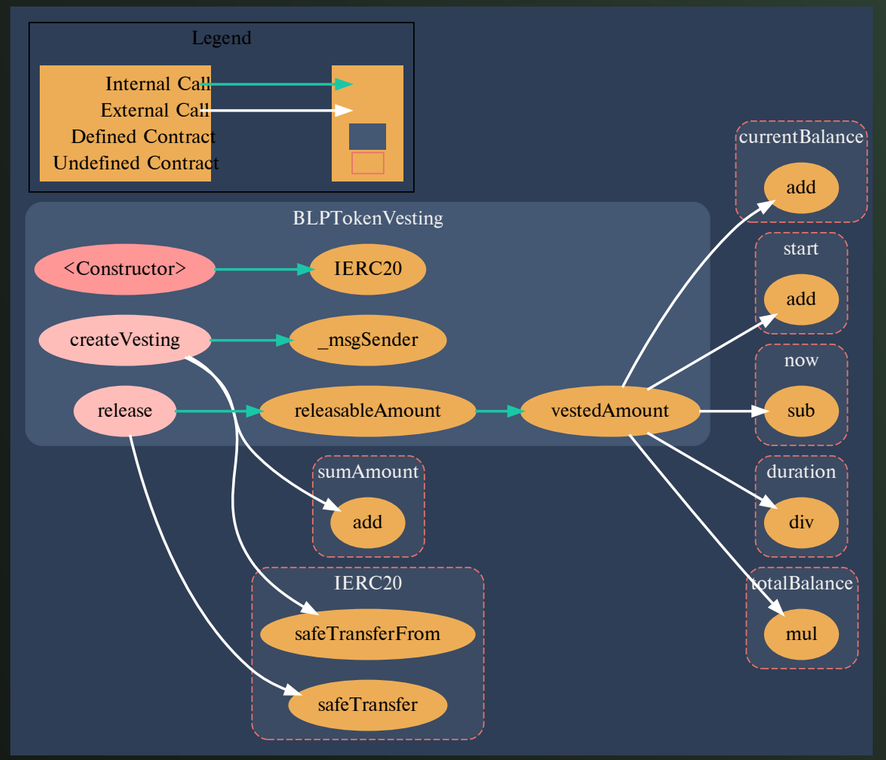
Contract methods analysis

createVesting(
address[] memory _users,
uint256[] memory _amounts
)
Vulnerabilities not detected

release(address _beneficiary)
Vulnerabilities not detected

releasableAmount(address _beneficiary)
Vulnerabilities not detected

vestedAmount(address _beneficiary)
Precision can be optimized the following way: totalBalance.
mul(now.sub(start)).div(totalIntervals



Pic.1.3.
BLPTokenVesting.sol

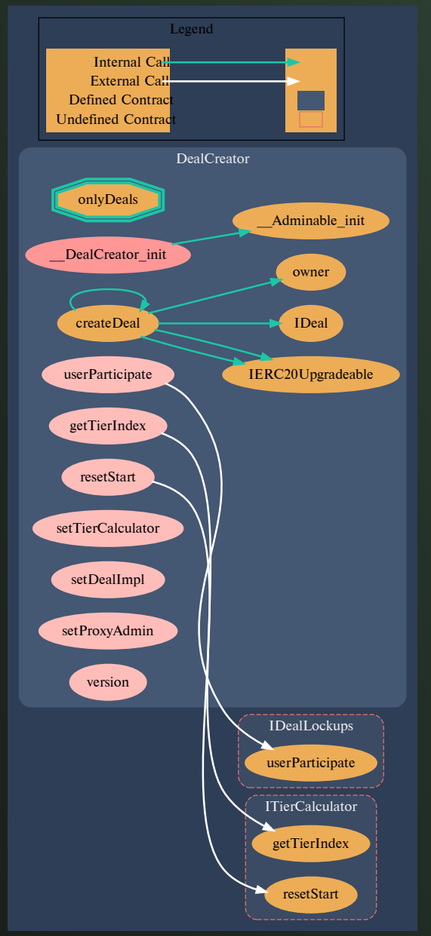
STRUCTURE OF CONTRACT
DEALCREATOR.SOL

Contract methods analysis

__DealCreator_init(
IDealLockups _dealLockups,
IVerifier _verifier,
ILocker _locker,
IVestingCreator _vestingCreator,
ITierCalculator _tierCalculator,
address _dealImpl,
address _proxyAdmin
)
Vulnerabilities not detected

createDeal(IDealCreator.DealInit memory _dealInit)
Vulnerabilities not detected

createDeal(IDealCreator.DealInit memory _dealInit, uint256 _decimalsRewardToken)
Vulnerabilities not detected



Pic.1.4.
DealCreator.sol

userParticipate(address _user, uint256 _tierIndex)
Vulnerabilities not detected

getTierIndex(address _user, address _deal)
Vulnerabilities not detected

resetStart(address _user)
Vulnerabilities not detected

setTierCalculator(ITierCalculator _tierCalculator)
Vulnerabilities not detected

setDealImpl(address _dealImpl)
Vulnerabilities not detected

setProxyAdmin(address _proxyAdmin)
Vulnerabilities not detected

version()
Vulnerabilities not detected

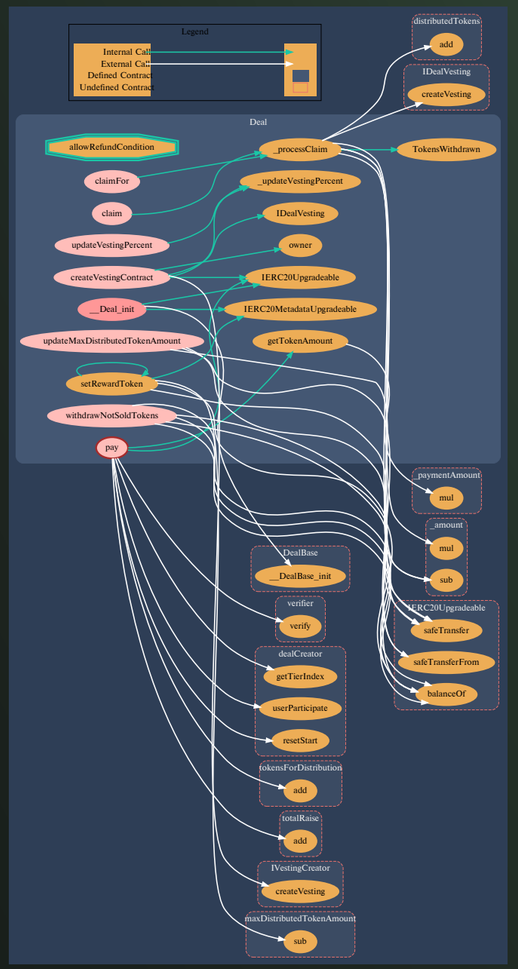
STRUCTURE OF CONTRACT
DEAL.SOL

Contract methods analysis

function __Deal_init(
IVerifier _verifier,
ILocker _locker,
IVestingCreator _vestingCreator,
IDealCreator.DealInit memory _dealInit,
uint256 _decimalsRewardToken,
address _dealCreator
)
Vulnerabilities not detected

function pay(uint256 _amount, bytes memory _signature)
Vulnerabilities not detected

getTokenAmount(uint256 _paymentAmount)
Vulnerabilities not detected



Pic.1.5.
Deal.sol

claimFor(address[] memory _addresses)
Vulnerabilities not detected

claim()
Vulnerabilities not detected

_processClaim(address _receiver)
Vulnerabilities not detected

withdrawNotSoldTokens(bool _emergency)
Vulnerabilities not detected

createVestingContract(
uint256 _percent,
uint256 _start,
uint256 _interval,
uint256 _duration
)
Vulnerabilities not detected

updateVestingPercent(uint256 _percent)
Vulnerabilities not detected

setRewardToken(IERC20Upgradeable _rewardToken)
Vulnerabilities not detected

setRewardToken(IERC20Upgradeable _rewardToken,
bool _checkDecimals)
Vulnerabilities not detected

_updateVestingPercent(uint256 _percent)
Vulnerabilities not detected

STRUCTURE OF CONTRACT
DEALBASE.SOL

Contract methods analysis

```
__DealBase_init(
      IVerifier _verifier,
      ILocker _locker,
      address _paymentToken,
      uint256 _tokenPrice,
      uint256 _startTimestamp,
      uint256 _finishTimestamp,
      uint256 _startClaimTimestamp,
      uint256 _minimumRaise,
      uint256 _maxDistributedTokenAmount,
      bool _allowRefund,
      address _dealCreator
    // uint256[] memory _tiersAmount
    )
```

Vulnerabilities not detected

Pic.1.6.
DealBase.sol

refund()
Vulnerabilities not detected

getTiersLength()
Vulnerabilities not detected

setTime(uint256 _startTimestamp, uint256 _finishTimestamp, uint256 _startClaimTimestamp)
Vulnerabilities not detected

_setTime(uint256 _startTimestamp, uint256 _finishTimestamp, uint256 _startClaimTimestamp)
Vulnerabilities not detected

withdrawFunds()
Vulnerabilities not detected

updateTier(uint256 _index, uint256 _blpAmount, uint256 _ticketSize, uint256 _allocation)
Vulnerabilities not detected

addTier(uint256 _blpAmount, uint256 _ticketSize, uint256 _allocation)
Vulnerabilities not detected

pause()
Vulnerabilities not detected

unpause()
Vulnerabilities not detected

checkExceedTiers()
Vulnerabilities not detected

STRUCTURE OF CONTRACT
DEALCOLLECTWALLET.SOL

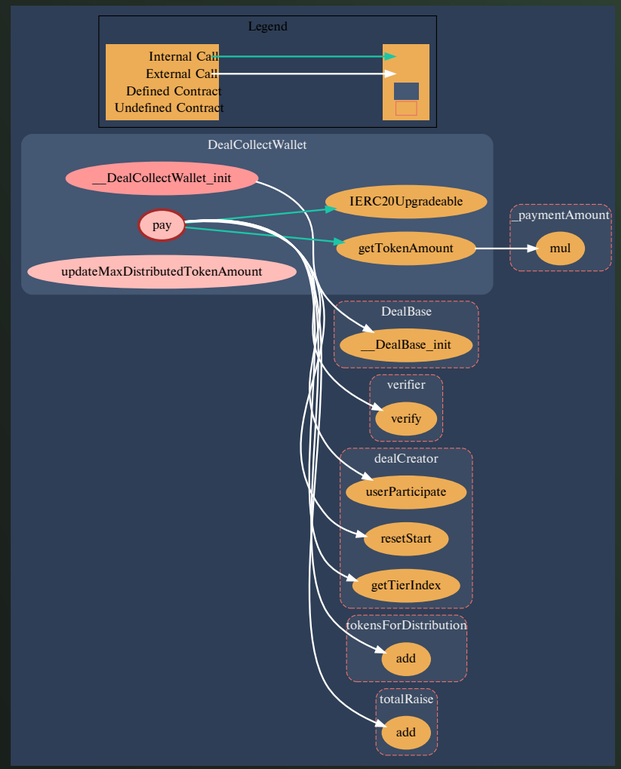
Contract methods analysis

__DealCollectWallet_init(
IVerifier _verifier,
ILocker _locker,
IDealCreator.WalletInit memory _walletInit,
address _dealCollectWalletCreator
)
Vulnerabilities not detected

pay(uint256 _amount, string memory _wallet, bytes memory _signature)
Vulnerabilities not detected

getTokenAmount(uint256 _paymentAmount)
Vulnerabilities not detected

updateMaxDistributedTokenAmount(uint256 _amount)
Vulnerabilities not detected



Pic.1.7.
DealCollectWallet.sol

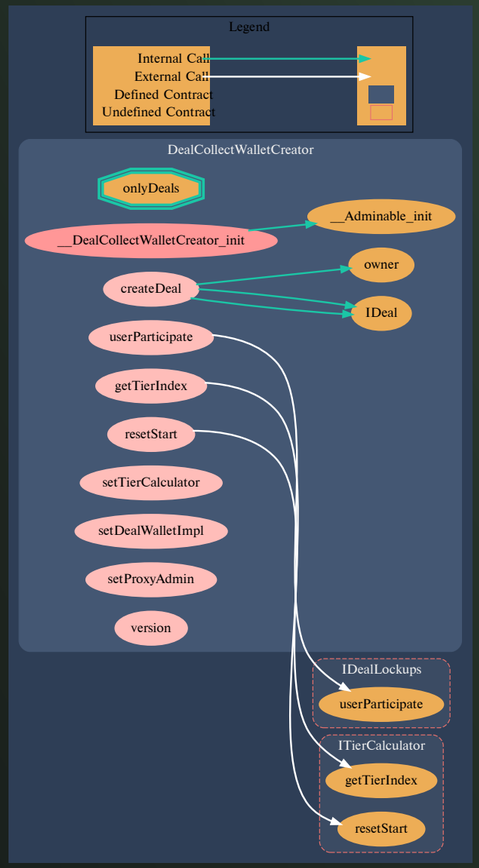
STRUCTURE OF CONTRACT
DEALCOLLECTWALLETCREATOR.SOL

Contract methods analysis

__DealCollectWalletCreator_init(
IDealLockups _dealLockups,
IVerifier _verifier,
ILocker _locker,
ITierCalculator _tierCalculator,
address _dealWalletImpl,
address _proxyAdmin
)
Vulnerabilities not detected

createDeal(IDealCreator.WalletInit memory _walletInit)
Vulnerabilities not detected

userParticipate(address _user, uint256 _tierIndex)
Vulnerabilities not detected



Pic.1.8.
DealCollectWalletCreator.sol

getTierIndex(address _user, address _deal)
Vulnerabilities not detected

resetStart(address _user)
Vulnerabilities not detected

setTierCalculator(ITierCalculator _tierCalculator)
Vulnerabilities not detected

setDealWalletImpl(address _dealWalletImpl)
Vulnerabilities not detected

setProxyAdmin(address _proxyAdmin)
Vulnerabilities not detected

STRUCTURE OF CONTRACT
DEALLOCKUPS.SOL

Contract methods analysis

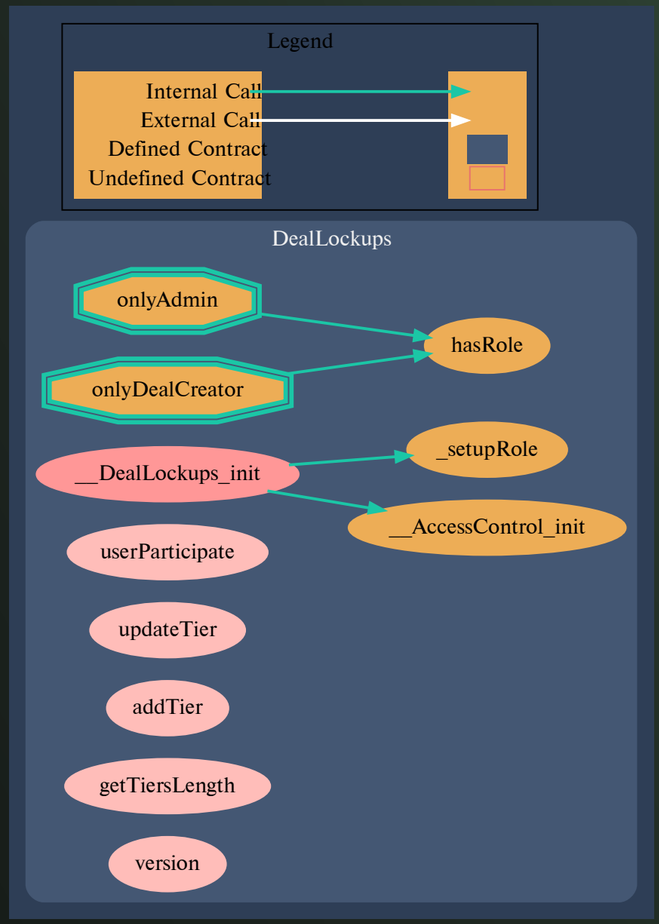
__DealLockups_init()
Vulnerabilities not detected

userParticipate(address _user, uint256 _tierIndex)
Vulnerabilities not detected

updateTier(uint256 _index, uint256 _blpAmount, uint256 _timeLockups)
Vulnerabilities not detected

addTier(uint256 _blpAmount, uint256 _timeLockups)
Vulnerabilities not detected

getTiersLength()
Vulnerabilities not detected



Pic.1.9.
DealLockups.sol

STRUCTURE OF CONTRACT
VESTINGCREATOR.SOL

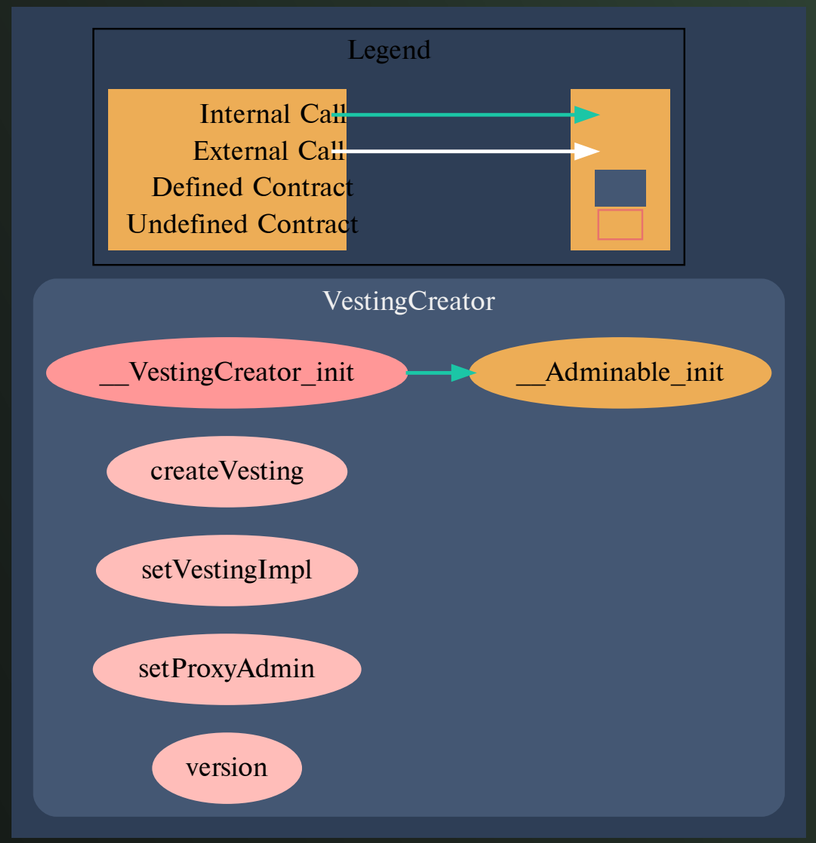
Contract methods analysis

__VestingCreator_init(address _vestingImpl, address _proxyAdmin)
Vulnerabilities not detected

createVesting(
address _dealAddress,
address _dealOwner,
IERC20Upgradeable _rewardToken,
uint256 _start,
uint256 _interval,
uint256 _duration
)
Vulnerabilities not detected

setVestingImpl(address _vestingImpl)
Vulnerabilities not detected

setProxyAdmin(address _proxyAdmin)
Vulnerabilities not detected



Pic.2.0.
VestingCreator.sol

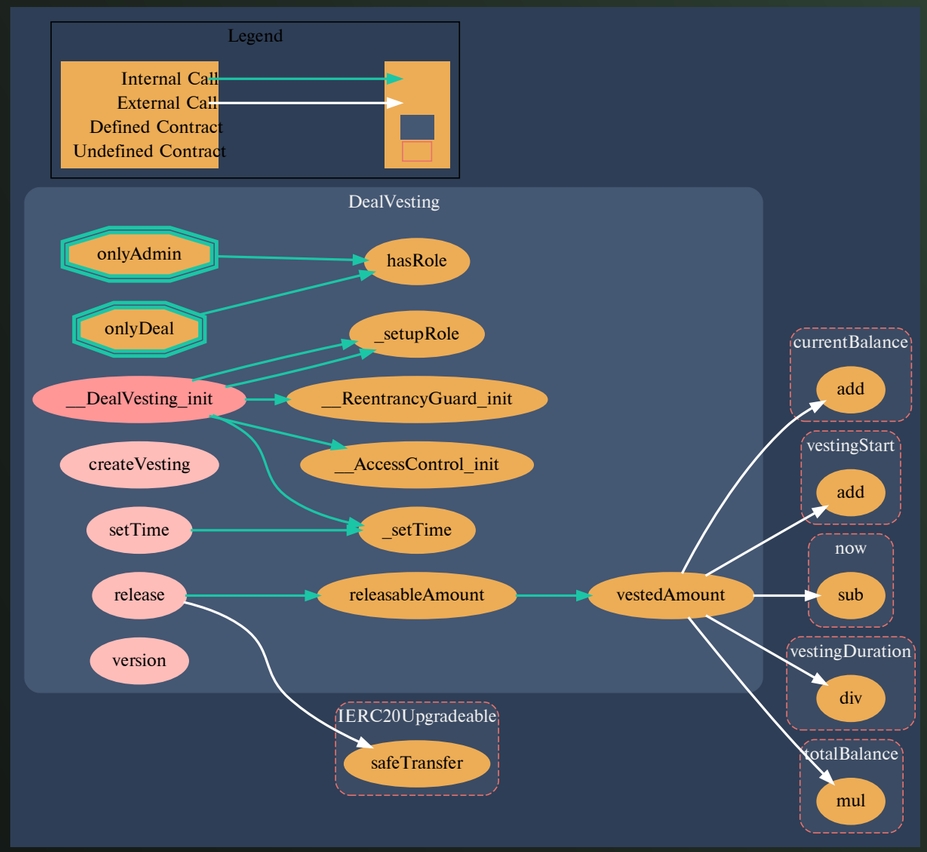
STRUCTURE OF CONTRACT
DEALVESTING.SOL

Contract methods analysis

__DealVesting_init(
address _dealAddress,
address _dealOwner,
IERC20Upgradeable _rewardToken,
uint256 _start,
uint256 _interval,
uint256 _duration)
Vulnerabilities not detected

createVesting(address _beneficiary, uint256 _amount)
Vulnerabilities not detected

release(address _beneficiary)
Vulnerabilities not detected



Pic.2.1.
DealVesting.sol

releasableAmount(address _beneficiary)
Vulnerabilities not detected

vestedAmount(address _beneficiary)
Precision can be optimized the following way: totalBalance.
mul(now.sub(start)).div(totalIntervals

setTime(uint256 _start, uint256 _interval, uint256 _duration)
Vulnerabilities not detected

_setTime(uint256 _start, uint256 _interval, uint256 _duration)
Vulnerabilities not detected

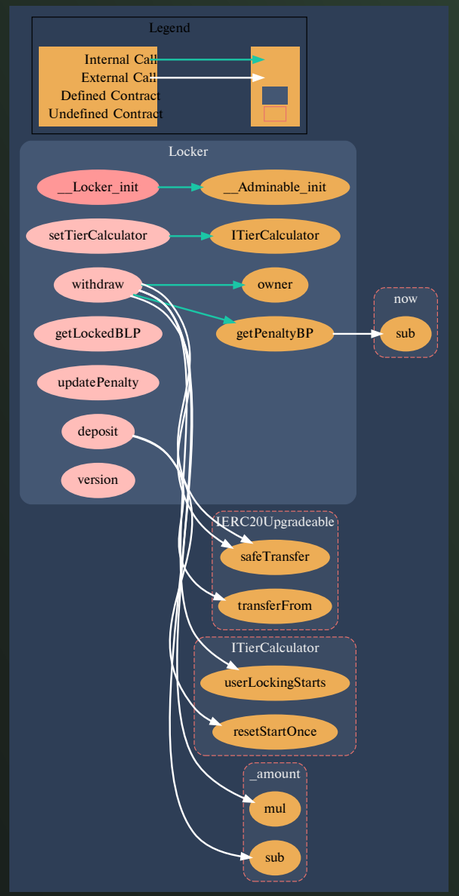
STRUCTURE OF CONTRACT
LOCKER.SOL

Contract methods analysis

__Locker_init(IERC20Upgradeable _blpToken, ITierCalculator _tierCalculator)
Vulnerabilities not detected

deposit(uint256 _amount)
Vulnerabilities not detected

withdraw(uint256 _amount)
Vulnerabilities not detected



Pic.2.2.
Locker.sol

getPenaltyBP(uint256 _startTime)
Vulnerabilities not detected

getLockedBLP(address _user)
Vulnerabilities not detected

updatePenalty(uint256 _index, uint256 _duration, uint256 _penaltyBP)
Vulnerabilities not detected

setTierCalculator(address _tierCalculator)
Vulnerabilities not detected

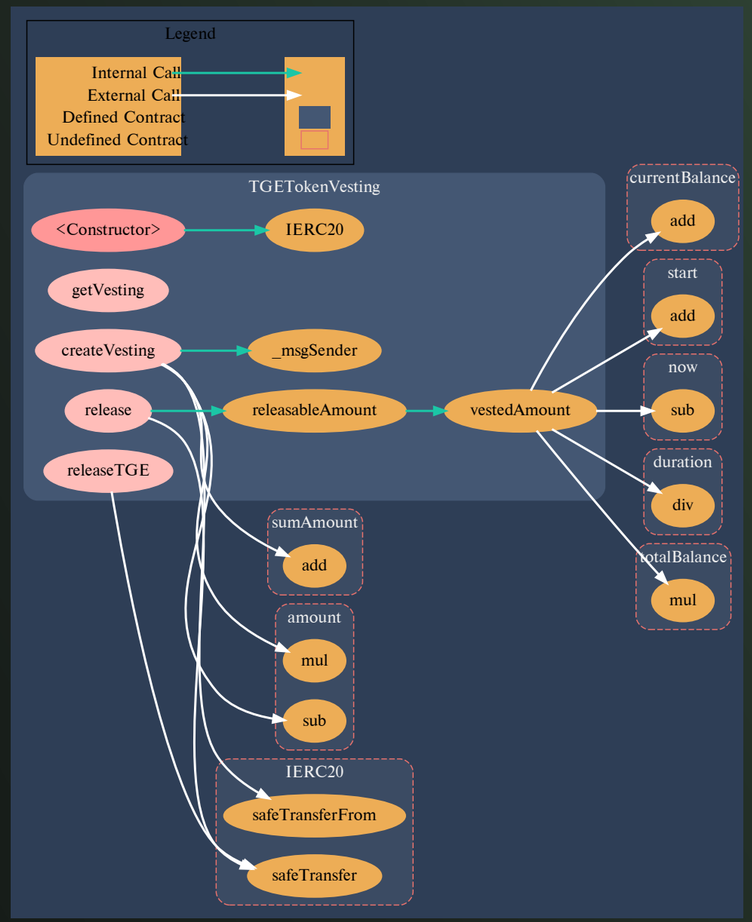
STRUCTURE OF CONTRACT
TGETOKENVESTING.SOL

Contract methods analysis

getVesting(address _beneficiary)
Vulnerabilities not detected

createVesting(
address[] memory _users,
uint256[] memory _amounts
)
Vulnerabilities not detected

releaseTGE(address _beneficiary)
Vulnerabilities not detected



Pic.2.3.
TGETokenVesting.sol

release(address _beneficiary)
Vulnerabilities not detected

releasableAmount(address _beneficiary)
Vulnerabilities not detected

vestedAmount(address _beneficiary)
Precision can be optimized the following way: totalBalance.
mul(now.sub(start)).div(totalIntervals

STRUCTURE OF CONTRACT
VERIFIER.SOL

Contract methods analysis

__Verifier_init(address _signWallet)
Vulnerabilities not detected

changeSigner(address _wallet)
Vulnerabilities not detected

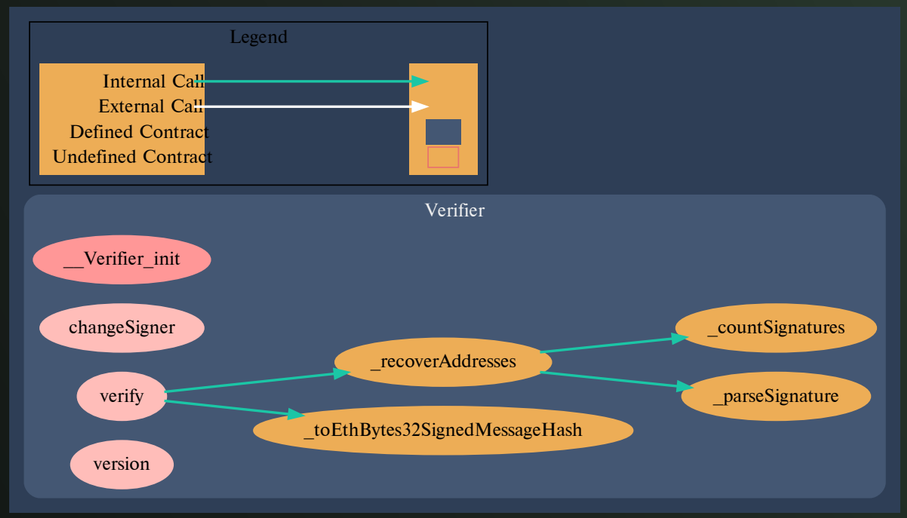
verify(bytes32 _message, bytes memory _signature)
Vulnerabilities not detected

_toEthBytes32SignedMessageHash (bytes32 _msg)
Vulnerabilities not detected

_recoverAddresses(bytes32 _hash, bytes memory _signatures)
Vulnerabilities not detected

_parseSignature(bytes memory _signatures, uint _pos)
Vulnerabilities not detected

_countSignatures(bytes memory _signatures)
Vulnerabilities not detected



Pic.2.4.
Verifier.sol

STRUCTURE OF CONTRACT
TIERCALCULATOR.SOL

Contract methods analysis

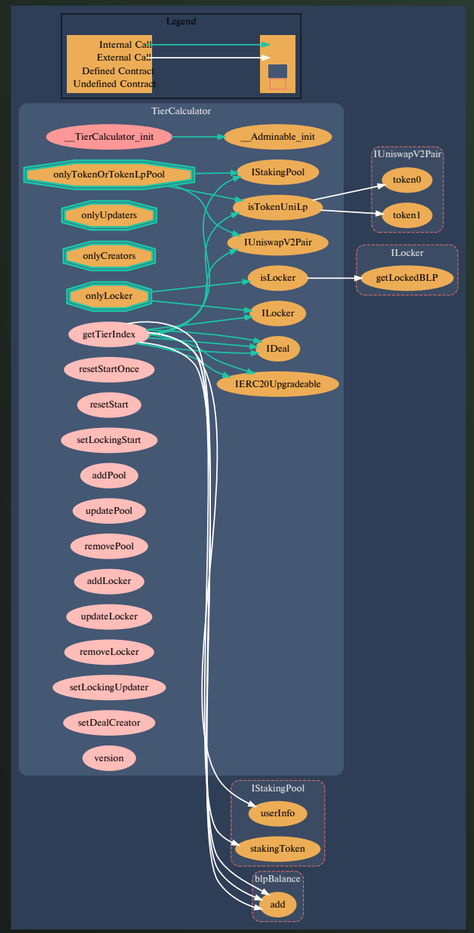
__TierCalculator_init(address _token)
Vulnerabilities not detected

getTierIndex(address _user, address _deal)
Vulnerabilities not detected

isTokenUniLp(IUniswapV2Pair _lp)
Vulnerabilities not detected

isLocker(ILocker _locker)
Vulnerabilities not detected

resetStartOnce(address _user)
Vulnerabilities not detected



Pic.2.5.
TierCalculator.sol

resetStart(address _user)
Vulnerabilities not detected

setLockingStart(address _user, uint256 _lockingStart)
Vulnerabilities not detected

addPool(address _pool)
Vulnerabilities not detected

updatePool(uint256 _index, address _pool)
Vulnerabilities not detected

removePool(uint256 _index)
Vulnerabilities not detected

addLocker(address _locker)
Vulnerabilities not detected

updateLocker(uint256 _index, address _locker)
Vulnerabilities not detected

removeLocker(uint256 _index)
Vulnerabilities not detected

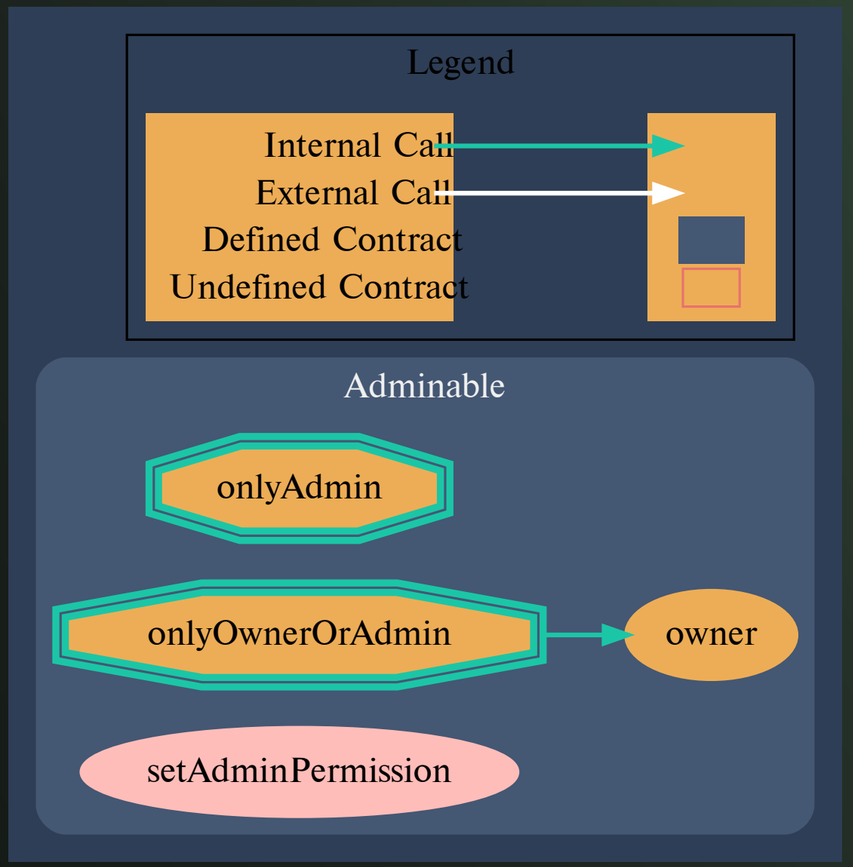
setLockingUpdater(address _lockingUpdater, bool _permission)
Vulnerabilities not detected

setDealCreator(address _dealCreator, bool _permission)
Vulnerabilities not detected

STRUCTURE OF CONTRACT
ADMINABLE.SOL

Contract methods analysis

setAdminPermission(address _user, bool _permission)
Vulnerabilities not detected



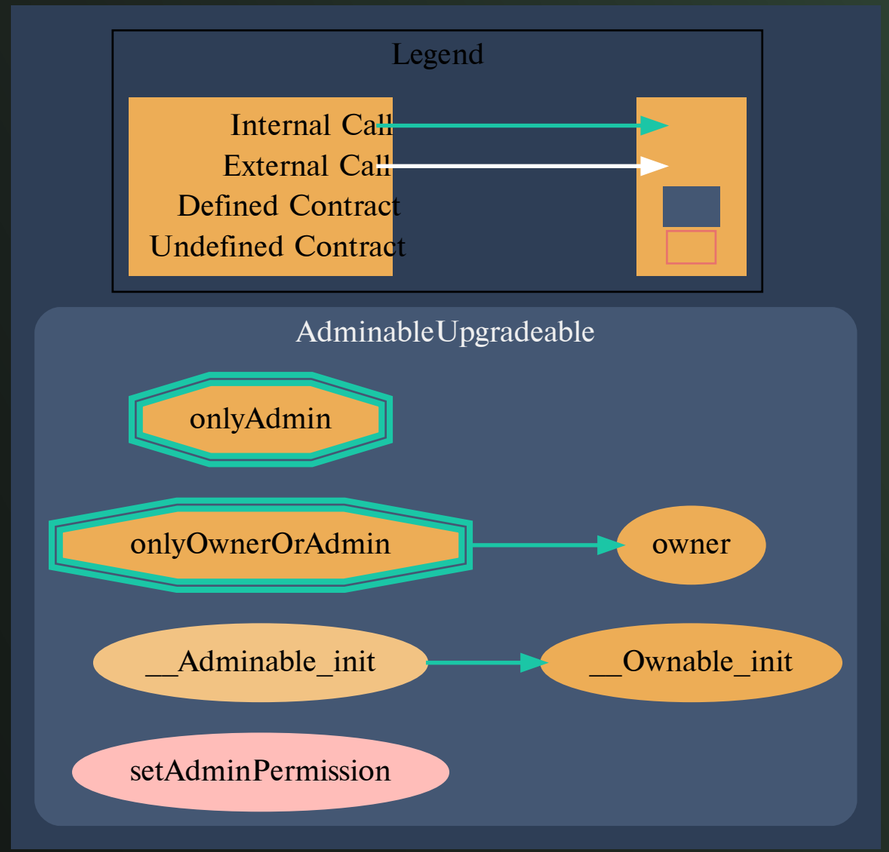
Pic.2.6.
Adminable.sol

STRUCTURE OF CONTRACT
ADMINABLEUPGRADEABLE.SOL

Contract methods analysis

__Adminable_init()
Vulnerabilities not detected

setAdminPermission(address _user, bool _permission)
Vulnerabilities not detected



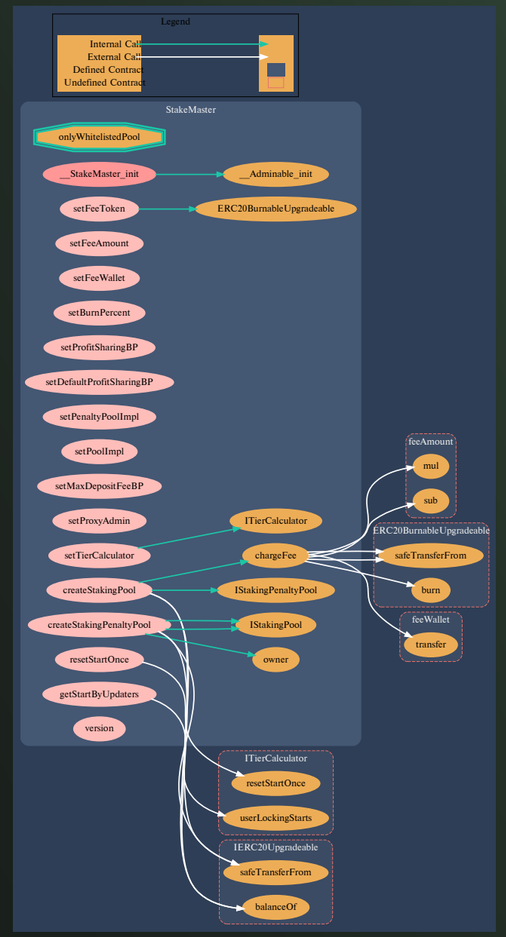
Pic.2.7.
AdminableUpgradeable.sol

STRUCTURE OF CONTRACT
STAKEMASTER.SOL

Contract methods analysis

```
__StakeMaster_init(
    ERC20BurnableUpgradeable _feeToken,
    address payable _feeWallet,
    uint256 _feeAmount,
    uint256 _burnPercent,
    uint256 _defaultProfitSharingBP,
    address _penaltyPoolImpl,
    address _poolImpl,
    uint256 _maxDepositFeeBP,
    address _proxyAdmin,
    ITierCalculator _tierCalculator
)
```

Vulnerabilities not detected



Pic.2.8.
StakeMaster.sol

setFeeToken(address _newFeeToken)
Vulnerabilities not detected

setFeeAmount(uint256 _newFeeAmount)
Reccomended to implement limits for feeAmount value

setFeeWallet(address payable _newFeeWallet)
Vulnerabilities not detected

setBurnPercent(uint256 _newBurnPercent, uint256 _newDivider)
Vulnerabilities not detected

setProfitSharingBP(address _stakingPool, uint256 _profitSharingBP)
Vulnerabilities not detected

setDefaultProfitSharingBP(uint256 _defaultProfitSharingBP)
Vulnerabilities not detected

setPenaltyPoolImpl(address _penaltyPoolImpl)
Vulnerabilities not detected

setPoolImpl(address _poolImpl)
Vulnerabilities not detected

setMaxDepositFeeBP(uint256 _maxDepositFeeBP)
Vulnerabilities not detected

setProxyAdmin(address _proxyAdmin)
Vulnerabilities not detected

setTierCalculator(address _tierCalculator)
Vulnerabilities not detected

resetStartOnce(address _user)
Vulnerabilities not detected

getStartByUpdaters(address _user)
Vulnerabilities not detected

createStakingPool(
IERC20Upgradeable _stakingToken,
IERC20Upgradeable _poolToken,
uint256 _startTime,
uint256 _finishTime,
uint256 _poolTokenAmount,
bool _hasWhitelisting,
uint256 _depositFeeBP,
address _feeTo
)
Vulnerabilities not detected

createStakingPenaltyPool(
IERC20Upgradeable _stakingToken,
IERC20Upgradeable _poolToken,
uint256 _startTime,
uint256 _finishTime,
uint256 _poolTokenAmount,
bool _hasWhitelisting,
uint256 _depositFeeBP,
address _feeTo
)
Vulnerabilities not detected

chargeFee()
Vulnerabilities not detected

STRUCTURE OF CONTRACT
WHITELISTUPGRADEABLE.SOL

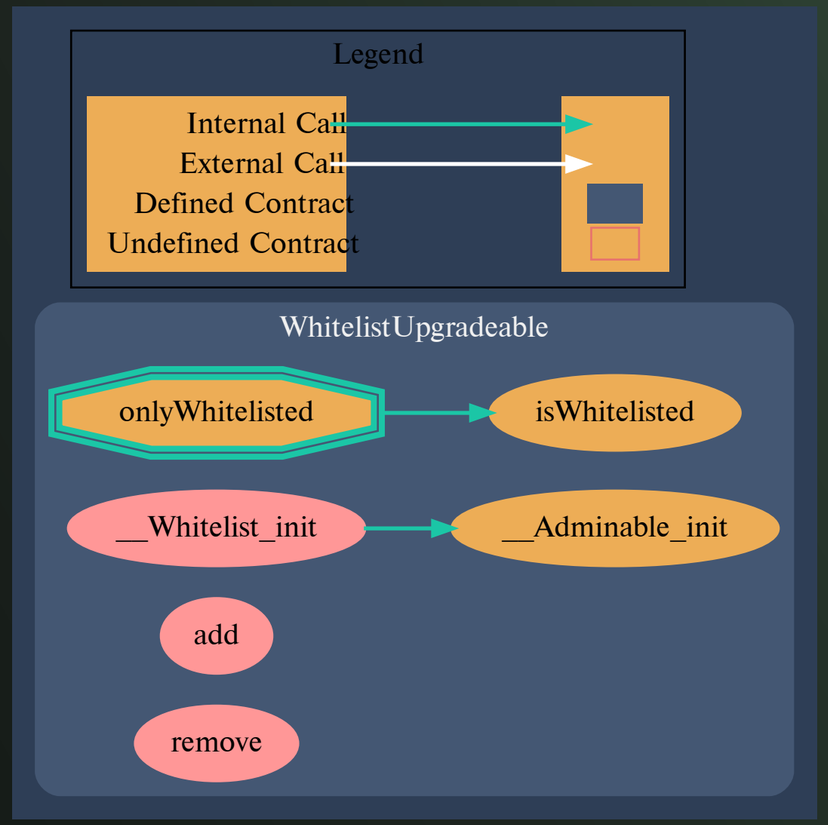
Contract methods analysis

__Whitelist_init (bool _hasWhitelisting)
Vulnerabilities not detected

add(address[] memory _addresses)
Vulnerabilities not detected

remove(address[] memory _addresses)
Method can be declared external

isWhitelisted(address _address)
Method can be declared external



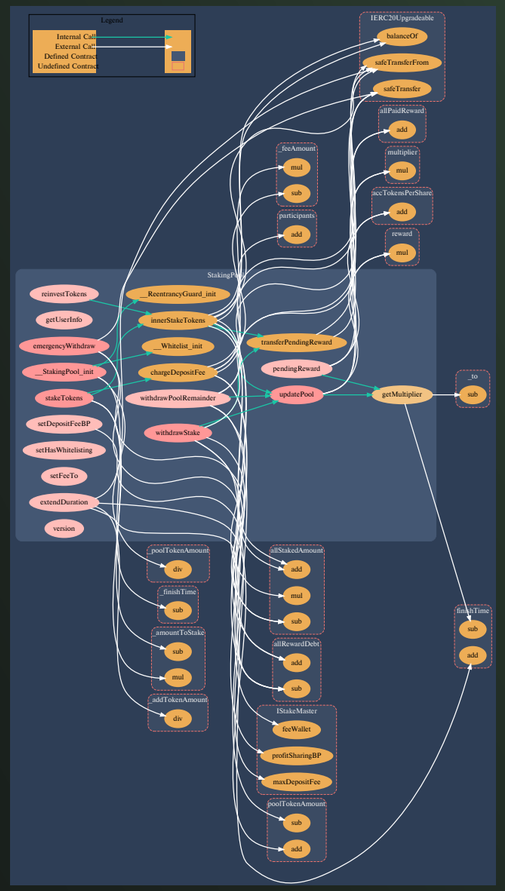
Pic.2.9.
WhitelistUpgradeable.sol

STRUCTURE OF CONTRACT
STAKINGPOOL.SOL

Contract methods analysis

__StakingPool_init(
    IERC20Upgradeable _stakingToken,
    IERC20Upgradeable _poolToken,
    uint256 _startTime,
    uint256 _finishTime,
    uint256 _poolTokenAmount,
    bool _hasWhitelisting,
    IStakeMaster _stakeMaster,
    uint256 _depositFeeBP,
    address _feeTo
)
Vulnerabilities not detected

getUserInfo(address user)
Vulnerabilities not detected



Pic.3.0.
StakingPool.sol

getMultiplier(uint256 _from, uint256 _to)
Vulnerabilities not detected

pendingReward(address _user)
Vulnerabilities not detected

updatePool()t)
Vulnerabilities not detected

reinvestTokens()
Vulnerabilities not detected

stakeTokens(uint256 _amountToStake)
Vulnerabilities not detected

chargeDepositFee(uint256 _feeAmount)
Vulnerabilities not detected

innerStakeTokens(uint256 _amountToStake, bool reinvest)
Vulnerabilities not detected

withdrawStake(uint256 _amount)
Vulnerabilities not detected

transferPendingReward(UserInfo memory user, bool reinvest)
Vulnerabilities not detected

emergencyWithdraw()
Vulnerabilities not detected

withdrawPoolRemainder()
Vulnerabilities not detected

extendDuration(uint256 _addTokenAmount)
Vulnerabilities not detected

setHasWhitelisting(bool value)
Vulnerabilities not detected

setFeeTo(address _feeTo)
Vulnerabilities not detected

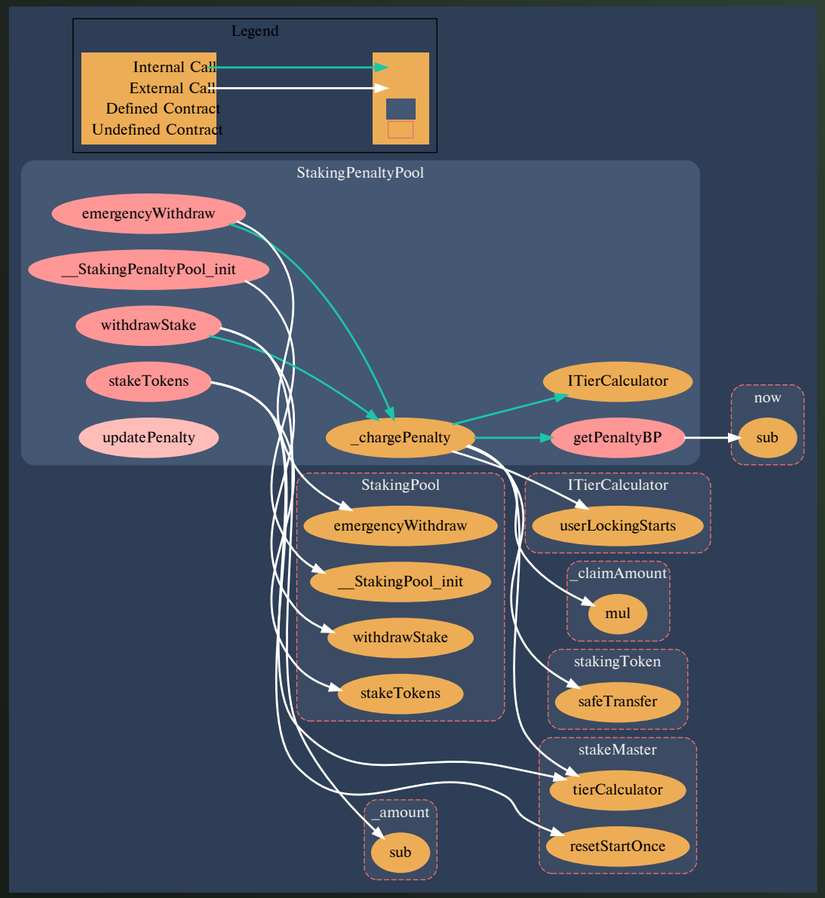
setDepositFeeBP(uint256 _depositFeeBP)
Vulnerabilities not detected

STRUCTURE OF CONTRACT
STAKINGPENALTYPOOL.SOL

Contract methods analysis

__StakingPenaltyPool_init(
    IERC20Upgradeable _stakingToken,
    IERC20Upgradeable _poolToken,
    uint256 _startTime,
    uint256 _finishTime,
    uint256 _poolTokenAmount,
    bool _hasWhitelisting,
    IStakeMaster _stakeMaster,
    uint256 _depositFeeBP,
    address _feeTo
)

Vulnerabilities not detected



Pic.3.1.
StakingPenaltyPool.sol

stakeTokens(uint256 _amountToStake)
Vulnerabilities not detected

withdrawStake(uint256 _amount)
Vulnerabilities not detected

emergencyWithdraw()
Vulnerabilities not detected

getPenaltyBP(uint256 _startTime)
Vulnerabilities not detected

updatePenalty(uint256 _index, uint256 _duration, uint256 _penaltyBP)
Vulnerabilities not detected

_chargePenalty(address _userAddress, uint256 _claimAmount)
Vulnerabilities not detected

GET IN TOUCH

info@smartstate.tech
smartstate.tech