ZEROSEC AUDIT REPORT

PROJECT NAME: MASTER KEY FINANCE

CONTRACT: MKFMARKET.SOL

WEBSITE: HTTPS://MASTERKEY.FINANCE

INTRODUCTION

Auditing Firm	Zero Sec LLC
Client Firm	Master Key Finance
Methodology	Manual and Automated Analysis
Language	Solidity
Contract	No Deployment Address
Blockchain	Binance Smart Chain
Ownership	Centralized Ownership
Website	https://masterkey.finance
Telegram	https://t.me/MasterKeyOfficial
Twitter	https://www.x.com/MasterKey_Fin
Instagram	https://instagram.com/mkf__official
Report Date	September 9, 2024

EXECUTIVE SUMMARY

Impact Level	Definition
Ad Hoc/Automated/High	The issue has a high impact on the contract's security and functionality.
Ad Hoc/Automated/Medium	The issue has a medium impact on the contract's security and functionality.
Ad Hoc/Automated/Low	The issue has a low impact on the contract's security and functionality.
Informational	The issue provides informational details but does not affect security or functionality.
Optimization	The issue relates to code optimization and does not affect security or functionality.

Impact Level	Count
Ad Hoc High	0
Automated High	8
Automated Medium	7
Automated Low	13
Automated Informational	63

Issue	arbitrary-send-eth
Type	node
Impact	High
Confidence	Medium
Name	(success) = feeCollector.call{value: address(this).balance}()
Source	MKFMarket.sol
Lines	405-405

MasterKeyPortalMarketplace.monthly() (MKFMarket.sol#393-408) sends eth to arbitrary user
Dangerous calls:
- (success) = feeCollector.call{value: address(this).balance}() (MKFMarket.sol#405)

function: monthly
Source: MKFMarket.sol
Lines: 393-408

node: (success) = feeCollector.call{value: address(this).balance}()
Source: MKFMarket.sol
Lines: 405-405

Issue	unchecked-transfer
Type	node
Impact	High
Confidence	Medium
Name	fromContract.transferFrom(msg.sender,address(this),fromAmount)
Source	MKFMarket.sol
Lines	263-263

MasterKeyPortalMarketplace.createListing(uint256,uint256,uint256,uint256) (MKFMarket.sol#236-288) ignores return value by fromContract.transferFrom(msg.sender,address(this),fromAmount) (MKFMarket.sol#263)

function: createListing
Source: MKFMarket.sol
Lines: 236-288

node: fromContract.transferFrom(msg.sender,address(this),fromAmount)
Source: MKFMarket.sol
Lines: 263-263

Issue	unchecked-transfer

Type	node
Impact	High
Confidence	Medium
Name	fromContract.transfer(msg.sender,targetListing.fromAmount)
Source	MKFMarket.sol
Lines	304-304

MasterKeyPortalMarketplace.buyListing(uint256) (MKFMarket.sol#290-318) ignores return value by fromContract.transfer(msg.sender,targetListing.fromAmount) (MKFMarket.sol#304)

function: buyListing
Source: MKFMarket.sol
Lines: 290-318

node: fromContract.transfer(msg.sender,targetListing.fromAmount)
Source: MKFMarket.sol
Lines: 304-304

Issue	**unchecked-transfer**
Type	node
Impact	High
Confidence	Medium
Name	tokenContract.transfer(msg.sender,_value)
Source	MKFMarket.sol
Lines	372-372

MasterKeyPortalMarketplace.emergencyWithdrawERC20(uint256,address) (MKFMarket.sol#369-373) ignores return value by tokenContract.transfer(msg.sender,_value) (MKFMarket.sol#372)

function: emergencyWithdrawERC20
Source: MKFMarket.sol
Lines: 369-373

node: tokenContract.transfer(msg.sender,_value)
Source: MKFMarket.sol
Lines: 372-372

Issue	**unchecked-transfer**
Type	node
Impact	High
Confidence	Medium

Name	IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt)
Source	MKFMarket.sol
Lines	398-398

MasterKeyPortalMarketplace.monthly() (MKFMarket.sol#393-408) ignores return value by IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt) (MKFMarket.sol#398)

function: monthly
Source: MKFMarket.sol
Lines: 393-408

node: IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt)
Source: MKFMarket.sol
Lines: 398-398

Issue	**unchecked-transfer**
Type	node
Impact	High
Confidence	Medium
Name	tokenContract.transfer(msg.sender,targetListing.fromAmount)
Source	MKFMarket.sol
Lines	328-328

MasterKeyPortalMarketplace.removeListing(uint256) (MKFMarket.sol#320-336) ignores return value by tokenContract.transfer(msg.sender,targetListing.fromAmount) (MKFMarket.sol#328)

function: removeListing
Source: MKFMarket.sol
Lines: 320-336

node: tokenContract.transfer(msg.sender,targetListing.fromAmount)
Source: MKFMarket.sol
Lines: 328-328

Issue	**unchecked-transfer**
Type	node
Impact	High
Confidence	Medium
Name	toContract.transferFrom(msg.sender,targetListing.listingAddress,targetListing.toAmount)
Source	MKFMarket.sol
Lines	306-306

MasterKeyPortalMarketplace.buyListing(uint256) (MKFMarket.sol#290-318) ignores return value by toContract.transferFrom(msg.sender,targetListing.listingAddress,targetListing.toAmount) (MKFMarket.sol#306)

function: buyListing
Source: MKFMarket.sol
Lines: 290-318

node: toContract.transferFrom(msg.sender,targetListing.listingAddress,targetListing.toAmount)
Source: MKFMarket.sol
Lines: 306-306

Issue	unchecked-transfer
Type	node
Impact	High
Confidence	Medium
Name	MSFY.transferFrom(address(this),msg.sender,claim.rewardsDebt)
Source	MKFMarket.sol
Lines	389-389

MasterKeyPortalMarketplace.claimReward() (MKFMarket.sol#387-391) ignores return value by MSFY.transferFrom(address(this),msg.sender,claim.rewardsDebt) (MKFMarket.sol#389)

function: claimReward
Source: MKFMarket.sol
Lines: 387-391

node: MSFY.transferFrom(address(this),msg.sender,claim.rewardsDebt)
Source: MKFMarket.sol
Lines: 389-389

Issue	divide-before-multiply
Type	node
Impact	Medium
Confidence	Medium
Name	bounty = targetListing.mkfBounty * dayselapsed
Source	MKFMarket.sol
Lines	344-344

MasterKeyPortalMarketplace.getListingBounty(uint256) (MKFMarket.sol#338-347) performs a multiplication on the result of a division:
- dayselapsed = ((currenttime - datelisted) / listingRewardTimeframe) (MKFMarket.sol#342)
- bounty = targetListing.mkfBounty * dayselapsed (MKFMarket.sol#344)

function: getListingBounty
Source: MKFMarket.sol
Lines: 338-347

node: dayselapsed = ((currenttime - datelisted) / listingRewardTimeframe)
Source: MKFMarket.sol
Lines: 342-342

node: bounty = targetListing.mkfBounty * dayselapsed
Source: MKFMarket.sol
Lines: 344-344

Issue	divide-before-multiply
Type	node
Impact	Medium
Confidence	Medium
Name	reward = targetListing.mkfReward * dayselapsed
Source	MKFMarket.sol
Lines	343-343

MasterKeyPortalMarketplace.getListingBounty(uint256) (MKFMarket.sol#338-347) performs a multiplication on the result of a division:
- dayselapsed = ((currenttime - datelisted) / listingRewardTimeframe) (MKFMarket.sol#342)
- reward = targetListing.mkfReward * dayselapsed (MKFMarket.sol#343)

function: getListingBounty
Source: MKFMarket.sol
Lines: 338-347

node: dayselapsed = ((currenttime - datelisted) / listingRewardTimeframe)
Source: MKFMarket.sol
Lines: 342-342

node: reward = targetListing.mkfReward * dayselapsed
Source: MKFMarket.sol
Lines: 343-343

Issue	reentrancy-no-eth
Type	node
Impact	Medium
Confidence	Medium
Name	delete listings[listingId]

Source	MKFMarket.sol
Lines	334-334

Reentrancy in MasterKeyPortalMarketplace.removeListing(uint256) (MKFMarket.sol#320-336):
External calls:
- tokenContract.transfer(msg.sender,targetListing.fromAmount) (MKFMarket.sol#328)
State variables written after the call(s):
- delete listings[listingId] (MKFMarket.sol#334)
MasterKeyPortalMarketplace.listings (MKFMarket.sol#66) can be used in cross function reentrancies:
- MasterKeyPortalMarketplace.getListingBounty(uint256) (MKFMarket.sol#338-347)
- MasterKeyPortalMarketplace.listings (MKFMarket.sol#66)

function: removeListing
Source: MKFMarket.sol
Lines: 320-336

node: tokenContract.transfer(msg.sender,targetListing.fromAmount)
Source: MKFMarket.sol
Lines: 328-328

node: delete listings[listingId]
Source: MKFMarket.sol
Lines: 334-334

Issue	**reentrancy-no-eth**
Type	node
Impact	Medium
Confidence	Medium
Name	rewards[msg.sender].rewardsDebt -= cost
Source	MKFMarket.sol
Lines	142-142

Reentrancy in MasterKeyPortalMarketplace.triggerRefillSubscription(uint256)
(MKFMarket.sol#137-144):
External calls:
- cost = subscriptionService.subscriptionPrice() (MKFMarket.sol#140)
State variables written after the call(s):
- rewards[msg.sender].rewardsDebt -= cost (MKFMarket.sol#142)
MasterKeyPortalMarketplace.rewards (MKFMarket.sol#67) can be used in cross function reentrancies:
- MasterKeyPortalMarketplace.rewards (MKFMarket.sol#67)
- MasterKeyPortalMarketplace.setrewardsDebt(address) (MKFMarket.sol#232-234)
- MasterKeyPortalMarketplace.triggerRefillSubscription(uint256) (MKFMarket.sol#137-144)
- MasterKeyPortalMarketplace.userRegister(address) (MKFMarket.sol#222-230)

function: triggerRefillSubscription
Source: MKFMarket.sol
Lines: 137-144

node: cost = subscriptionService.subscriptionPrice()
Source: MKFMarket.sol
Lines: 140-140

node: rewards[msg.sender].rewardsDebt -= cost
Source: MKFMarket.sol
Lines: 142-142

Issue	reentrancy-no-eth
Type	node
Impact	Medium
Confidence	Medium
Name	delete listings[listingId]
Source	MKFMarket.sol
Lines	315-315

Reentrancy in MasterKeyPortalMarketplace.buyListing(uint256) (MKFMarket.sol#290-318):
External calls:
- fromContract.transfer(msg.sender,targetListing.fromAmount) (MKFMarket.sol#304)
- toContract.transferFrom(msg.sender,targetListing.listingAddress,targetListing.toAmount)
(MKFMarket.sol#306)
State variables written after the call(s):
- delete listings[listingId] (MKFMarket.sol#315)
MasterKeyPortalMarketplace.listings (MKFMarket.sol#66) can be used in cross function reentrancies:
- MasterKeyPortalMarketplace.getListingBounty(uint256) (MKFMarket.sol#338-347)
- MasterKeyPortalMarketplace.listings (MKFMarket.sol#66)

function: buyListing
Source: MKFMarket.sol
Lines: 290-318

node: fromContract.transfer(msg.sender,targetListing.fromAmount)
Source: MKFMarket.sol
Lines: 304-304

node: toContract.transferFrom(msg.sender,targetListing.listingAddress,targetListing.toAmount)
Source: MKFMarket.sol
Lines: 306-306

node: delete listings[listingId]
Source: MKFMarket.sol
Lines: 315-315

Issue	reentrancy-no-eth

Type	node
Impact	Medium
Confidence	Medium
Name	token.taxDebt = 0
Source	MKFMarket.sol
Lines	400-400

Reentrancy in MasterKeyPortalMarketplace.monthly() (MKFMarket.sol#393-408):
External calls:
- IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt) (MKFMarket.sol#398)
State variables written after the call(s):
- token.taxDebt = 0 (MKFMarket.sol#400)
MasterKeyPortalMarketplace.tokens (MKFMarket.sol#64) can be used in cross function reentrancies:
- MasterKeyPortalMarketplace.addWhitelistToken(address,string,uint256) (MKFMarket.sol#187-214)
- MasterKeyPortalMarketplace.monthly() (MKFMarket.sol#393-408)
- MasterKeyPortalMarketplace.setTaxRate(uint256,uint256) (MKFMarket.sol#183-185)
- MasterKeyPortalMarketplace.tokens (MKFMarket.sol#64)

function: monthly
Source: MKFMarket.sol
Lines: 393-408

node: IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt)
Source: MKFMarket.sol
Lines: 398-398

node: token.taxDebt = 0
Source: MKFMarket.sol
Lines: 400-400

Issue	**reentrancy-no-eth**
Type	node
Impact	Medium
Confidence	Medium
Name	rewards[msg.sender].rewardsDebt = 0
Source	MKFMarket.sol
Lines	390-390

Reentrancy in MasterKeyPortalMarketplace.claimReward() (MKFMarket.sol#387-391):
External calls:
- MSFY.transferFrom(address(this),msg.sender,claim.rewardsDebt) (MKFMarket.sol#389)
State variables written after the call(s):
- rewards[msg.sender].rewardsDebt = 0 (MKFMarket.sol#390)
MasterKeyPortalMarketplace.rewards (MKFMarket.sol#67) can be used in cross function reentrancies:
- MasterKeyPortalMarketplace.rewards (MKFMarket.sol#67)

- MasterKeyPortalMarketplace.setrewardsDebt(address) (MKFMarket.sol#232-234)
- MasterKeyPortalMarketplace.triggerRefillSubscription(uint256) (MKFMarket.sol#137-144)
- MasterKeyPortalMarketplace.userRegister(address) (MKFMarket.sol#222-230)

function: claimReward
Source: MKFMarket.sol
Lines: 387-391

node: MSFY.transferFrom(address(this),msg.sender,claim.rewardsDebt)
Source: MKFMarket.sol
Lines: 389-389

node: rewards[msg.sender].rewardsDebt = 0
Source: MKFMarket.sol
Lines: 390-390

Issue	events-access
Type	node
Impact	Low
Confidence	Medium
Name	authorizedContract = _newAddress
Source	MKFMarket.sol
Lines	134-134

MasterKeyPortalMarketplace.updateSubscriptionServiceAddress(address) (MKFMarket.sol#132-135)
should emit an event for:
- authorizedContract = _newAddress (MKFMarket.sol#134)

function: updateSubscriptionServiceAddress
Source: MKFMarket.sol
Lines: 132-135

node: authorizedContract = _newAddress
Source: MKFMarket.sol
Lines: 134-134

Issue	events-maths
Type	node
Impact	Low
Confidence	Medium
Name	BNBListingFee = _value
Source	MKFMarket.sol

Lines	164-164

MasterKeyPortalMarketplace.setBNBListingFee(int256) (MKFMarket.sol#163-165) should emit an event for:
- BNBListingFee = _value (MKFMarket.sol#164)

function: setBNBListingFee
Source: MKFMarket.sol
Lines: 163-165

node: BNBListingFee = _value
Source: MKFMarket.sol
Lines: 164-164

Issue	events-maths
Type	node
Impact	Low
Confidence	Medium
Name	listingRewardTimeframe = _value
Source	MKFMarket.sol
Lines	172-172

MasterKeyPortalMarketplace.setListingRewardTimeframe(uint256) (MKFMarket.sol#171-173) should emit an event for:
- listingRewardTimeframe = _value (MKFMarket.sol#172)

function: setListingRewardTimeframe
Source: MKFMarket.sol
Lines: 171-173

node: listingRewardTimeframe = _value
Source: MKFMarket.sol
Lines: 172-172

Issue	missing-zero-check
Type	node
Impact	Low
Confidence	Medium
Name	feeCollector = address(_value)
Source	MKFMarket.sol
Lines	180-180

MasterKeyPortalMarketplace.setFeeCollectorAddress(address)._value (MKFMarket.sol#179) lacks a zero-check on :
- feeCollector = address(_value) (MKFMarket.sol#180)

variable: _value
Source: MKFMarket.sol
Lines: 179-179

node: feeCollector = address(_value)
Source: MKFMarket.sol
Lines: 180-180

Issue	missing-zero-check
Type	node
Impact	Low
Confidence	Medium
Name	authorizedContract = _newAddress
Source	MKFMarket.sol
Lines	134-134

MasterKeyPortalMarketplace.updateSubscriptionServiceAddress(address)._newAddress (MKFMarket.sol#132) lacks a zero-check on :
- authorizedContract = _newAddress (MKFMarket.sol#134)

variable: _newAddress
Source: MKFMarket.sol
Lines: 132-132

node: authorizedContract = _newAddress
Source: MKFMarket.sol
Lines: 134-134

Issue	missing-zero-check
Type	node
Impact	Low
Confidence	Medium
Name	BBB = address(_value)
Source	MKFMarket.sol
Lines	176-176

MasterKeyPortalMarketplace.setBBBAddress(address)._value (MKFMarket.sol#175) lacks a zero-check on :
- BBB = address(_value) (MKFMarket.sol#176)

variable: _value
Source: MKFMarket.sol
Lines: 175-175

node: BBB = address(_value)
Source: MKFMarket.sol
Lines: 176-176

Issue	calls-loop
Type	node
Impact	Low
Confidence	Medium
Name	IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt)
Source	MKFMarket.sol
Lines	398-398

MasterKeyPortalMarketplace.monthly() (MKFMarket.sol#393-408) has external calls inside a loop:
IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt) (MKFMarket.sol#398)

function: monthly
Source: MKFMarket.sol
Lines: 393-408

node: IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt)
Source: MKFMarket.sol
Lines: 398-398

Issue	reentrancy-benign
Type	node
Impact	Low
Confidence	Medium
Name	rewards[msg.sender].rewardsDebt += reward
Source	MKFMarket.sol
Lines	332-332

Reentrancy in MasterKeyPortalMarketplace.removeListing(uint256) (MKFMarket.sol#320-336):
External calls:
- tokenContract.transfer(msg.sender,targetListing.fromAmount) (MKFMarket.sol#328)
State variables written after the call(s):
- rewards[msg.sender].rewardsDebt += reward (MKFMarket.sol#332)

function: removeListing
Source: MKFMarket.sol
Lines: 320-336

node: tokenContract.transfer(msg.sender,targetListing.fromAmount)
Source: MKFMarket.sol
Lines: 328-328

node: tokenContract.transfer(msg.sender,targetListing.fromAmount)
Source: MKFMarket.sol
Lines: 328-328

node: rewards[msg.sender].rewardsDebt += reward
Source: MKFMarket.sol
Lines: 332-332

Issue	reentrancy-benign
Type	node
Impact	Low
Confidence	Medium
Name	rewards[targetListing.listingAddress].rewardsDebt += reward
Source	MKFMarket.sol
Lines	312-312

Reentrancy in MasterKeyPortalMarketplace.buyListing(uint256) (MKFMarket.sol#290-318):
External calls:
- fromContract.transfer(msg.sender,targetListing.fromAmount) (MKFMarket.sol#304)
- toContract.transferFrom(msg.sender,targetListing.listingAddress,targetListing.toAmount)
(MKFMarket.sol#306)
State variables written after the call(s):
- rewards[msg.sender].rewardsDebt += bounty (MKFMarket.sol#309)
- rewards[targetListing.listingAddress].rewardsDebt += reward (MKFMarket.sol#312)

function: buyListing
Source: MKFMarket.sol
Lines: 290-318

node: fromContract.transfer(msg.sender,targetListing.fromAmount)
Source: MKFMarket.sol
Lines: 304-304

node: toContract.transferFrom(msg.sender,targetListing.listingAddress,targetListing.toAmount)
Source: MKFMarket.sol
Lines: 306-306

node: fromContract.transfer(msg.sender,targetListing.fromAmount)
Source: MKFMarket.sol
Lines: 304-304

node: toContract.transferFrom(msg.sender,targetListing.listingAddress,targetListing.toAmount)
Source: MKFMarket.sol
Lines: 306-306

node: rewards[msg.sender].rewardsDebt += bounty
Source: MKFMarket.sol
Lines: 309-309

node: rewards[targetListing.listingAddress].rewardsDebt += reward
Source: MKFMarket.sol
Lines: 312-312

Issue	reentrancy-benign
Type	node
Impact	Low
Confidence	Medium
Name	listingId = totalListings ++
Source	MKFMarket.sol
Lines	270-270

Reentrancy in MasterKeyPortalMarketplace.createListing(uint256,uint256,uint256,uint256)
(MKFMarket.sol#236-288):
External calls:
- fromContract.transferFrom(msg.sender,address(this),fromAmount) (MKFMarket.sol#263)
State variables written after the call(s):
- listings[listingId] = newListing (MKFMarket.sol#285)
- listingId = totalListings ++ (MKFMarket.sol#270)

function: createListing
Source: MKFMarket.sol
Lines: 236-288

node: fromContract.transferFrom(msg.sender,address(this),fromAmount)
Source: MKFMarket.sol
Lines: 263-263

node: fromContract.transferFrom(msg.sender,address(this),fromAmount)
Source: MKFMarket.sol
Lines: 263-263

node: listings[listingId] = newListing
Source: MKFMarket.sol
Lines: 285-285

node: listingId = totalListings ++
Source: MKFMarket.sol
Lines: 270-270

Issue	reentrancy-events
Type	node
Impact	Low
Confidence	Medium
Name	TaxTransfered(token.tokenId,token.taxDebt)
Source	MKFMarket.sol
Lines	399-399

Reentrancy in MasterKeyPortalMarketplace.monthly() (MKFMarket.sol#393-408):
External calls:
- IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt) (MKFMarket.sol#398)
Event emitted after the call(s):
- TaxTransfered(token.tokenId,token.taxDebt) (MKFMarket.sol#399)

function: monthly
Source: MKFMarket.sol
Lines: 393-408

node: IERC20extended(token.tokenAddress).transfer(feeCollector,token.taxDebt)
Source: MKFMarket.sol
Lines: 398-398

node: TaxTransfered(token.tokenId,token.taxDebt)
Source: MKFMarket.sol
Lines: 399-399

Issue	timestamp
Type	node
Impact	Low
Confidence	Medium
Name	reward > 0
Source	MKFMarket.sol
Lines	311-311

MasterKeyPortalMarketplace.buyListing(uint256) (MKFMarket.sol#290-318) uses timestamp for comparisons
Dangerous comparisons:
- require(bool,string)(listings[listingId].enabled == true,!IsListed) (MKFMarket.sol#294)
- bounty > 0 (MKFMarket.sol#308)
- reward > 0 (MKFMarket.sol#311)

function: buyListing
Source: MKFMarket.sol
Lines: 290-318

node: require(bool,string)(listings[listingId].enabled == true,!IsListed)
Source: MKFMarket.sol
Lines: 294-294

node: bounty > 0
Source: MKFMarket.sol
Lines: 308-308

node: reward > 0
Source: MKFMarket.sol
Lines: 311-311

Issue	timestamp
Type	node
Impact	Low
Confidence	Medium
Name	reward > 0
Source	MKFMarket.sol
Lines	331-331

MasterKeyPortalMarketplace.removeListing(uint256) (MKFMarket.sol#320-336) uses timestamp for comparisons
Dangerous comparisons:
- reward > 0 (MKFMarket.sol#331)

function: removeListing
Source: MKFMarket.sol
Lines: 320-336

node: reward > 0
Source: MKFMarket.sol
Lines: 331-331