Smart Contract
Security Audit Report

Table Of Contents

1 Executive Summary

On 2023.10.18, the SlowMist security team received the SpaceID team's security audit application for SpaceID Toolkit, developed the audit plan according to the agreement of both parties and the characteristics of the project, and finally issued the security audit report.

The SlowMist security team adopts the strategy of "white box lead, black, grey box assists" to conduct a complete security test on the project in the way closest to the real attack.

The test method information:

Test method	Description
Black box testing	Conduct security tests from an attacker's perspective externally.
Grey box testing	Conduct security testing on code modules through the scripting tool, observing the internal running status, mining weaknesses.
White box testing	Based on the open source code, non-open source code, to detect whether there are vulnerabilities in programs such as nodes, SDK, etc.

The vulnerability severity level information:

Level	Description
Critical	Critical severity vulnerabilities will have a significant impact on the security of the DeFi project, and it is strongly recommended to fix the critical vulnerabilities.
High	High severity vulnerabilities will affect the normal operation of the DeFi project. It is strongly recommended to fix high-risk vulnerabilities.
Medium	Medium severity vulnerability will affect the operation of the DeFi project. It is recommended to fix medium-risk vulnerabilities.
Low	Low severity vulnerabilities may affect the operation of the DeFi project in certain scenarios. It is suggested that the project team should evaluate and consider whether these vulnerabilities need to be fixed.
Weakness	There are safety risks theoretically, but it is extremely difficult to reproduce in engineering.
Suggestion	There are better practices for coding or architecture.

2 Audit Methodology

The security audit process of SlowMist security team for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using automated analysis tools.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that was considered during the audit of the smart contract:

Serial Number	Audit Class	Audit Subclass
1	Overflow Audit	-
2	Reentrancy Attack Audit	-
3	Replay Attack Audit	-
4	Flashloan Attack Audit	-
5	Race Conditions Audit	Reordering Attack Audit
6	Permission Vulnerability Audit	Access Control Audit
		Excessive Authority Audit
7	Security Design Audit	External Module Safe Use Audit
		Compiler Version Security Audit
		Hard-coded Address Security Audit
		Fallback Function Safe Use Audit
		Show Coding Security Audit
		Function Return Value Security Audit
		External Call Function Security Audit

Serial Number	Audit Class	Audit Subclass
7	Security Design Audit	Block data Dependence Security Audit
		tx.origin Authentication Security Audit
8	Denial of Service Audit	-
9	Gas Optimization Audit	-
10	Design Logic Audit	-
11	Variable Coverage Vulnerability Audit	-
12	"False Top-up" Vulnerability Audit	-
13	Scoping and Declarations Audit	-
14	Malicious Event Log Audit	-
15	Arithmetic Accuracy Deviation Audit	-
16	Uninitialized Storage Pointer Audit	-

3 Project Overview

3.1 Project Introduction

SPACE ID is building a universal name service network with a one-stop identity platform to discover, register, trade, manage web3 domains.

3.2 Vulnerability Information

The following is the status of the vulnerabilities found in this audit:

NO	Title	Category	Level	Status
N1	Missing event record	Malicious Event Log Audit	Suggestion	Confirming

NO	Title	Category	Level	Status
N2	Existence of unused variables	Others	Suggestion	Confirming
N3	Redundant code	Others	Suggestion	Confirming
N4	Risk of excessive authority	Authority Control Vulnerability Audit	Medium	Confirming
N5	Lack of reasonable scope limitations	Others	Suggestion	Confirming
N6	Missing zero address validation	Others	Low	Confirming
N7	Missing check for identifier	Others	Low	Confirming
N8	Preemptive Initialization	Race Conditions Vulnerability	Suggestion	Confirming

4 Code Overview

4.1 Contracts Description

https://github.com/Space-ID/spaceid-toolkit-audit

cc6fafaac3f246ace4c2a6b24f65252057580a62

Audit scope:

- contracts/access
- contracts/admin
- contracts/base
- contracts/common
- contracts/controller
- contracts/giftcard
- contracts/hook
- contracts/price-oracle
- contracts/proxy

- contracts/referral
- contracts/registrar
- contracts/registry

The main network address of the contract is as follows:

The code was not deployed to the mainnet.

4.2 Visibility Description

The SlowMist Security team analyzed the visibility of major contracts during the audit, the result as follows:

TreasuryAccessable			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	-

TreasuryAccessableUpgradeable			
Function Name	Visibility	Mutability	Modifiers
__TreasuryAccessable_init	Internal	Can Modify State	onlyInitializing

PlatformConfig			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
setDefaultMinPlatformFee	External	Can Modify State	onlyPlatformAdmin
setDefaultRateBps	External	Can Modify State	onlyPlatformAdmin
setPlatformFeeCollector	External	Can Modify State	onlyPlatformAdmin
setCustomizedPlatformFee	External	Can Modify State	onlyPlatformAdmin
computePlatformFee	Public	-	-
computeBasicPlatformFee	Public	-	-

PlatformConfig			
getMinPlatformFee	Public	-	-
getPlatformFeeRateBps	Public	-	-

PrepaidPlatformFee			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable TreasuryAccessable
deposit	External	Payable	-
deduct	External	Can Modify State	onlyTldController
withdraw	External	Can Modify State	onlyPlatformFeeCollector

SANN			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	-
initialize	External	Can Modify State	initializer
_authorizeUpgrade	Internal	Can Modify State	onlyPlatformAdmin
setTldFactory	External	Can Modify State	onlyPlatformAdmin
setPlatformAdmin	External	Can Modify State	onlyPlatformAdmin
setMinTldLength	External	Can Modify State	onlyPlatformAdmin
setMaxTldLength	External	Can Modify State	onlyPlatformAdmin
setTldController	External	Can Modify State	onlyPlatformAdmin
tld	External	-	-
tldOwner	Public	-	-
tldController	Public	-	-
tldBase	Public	-	-

SANN

tldIdentifier	Public	-	-
registerTld	External	Can Modify State	onlyValidTldFactory
transferNodeOwner	External	Can Modify State	onlyPlatformAdmin
setTldOwner	External	Can Modify State	onlyTldOwner
_isValidTld	Internal	-	-

TldFactory

Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
createDomainService	External	Can Modify State	onlyPlatformAdmin
_setPriceModel	Private	Can Modify State	-
_enableQualificationHook	Private	Can Modify State	-
_enablePreRegistration	Private	Can Modify State	-
_enablePriceHook	Private	Can Modify State	-
_enableGiftCard	Private	Can Modify State	-
_enableReferral	Private	Can Modify State	-
setDefaultPriceOracle	External	Can Modify State	onlyPlatformAdmin

Base

Function Name	Visibility	Mutability	Modifiers
_isApprovedOrOwner	Internal	-	-
<Constructor>	Public	Can Modify State	ERC721 TldAccessable
totalSupply	External	-	-

Base			
_mint	Internal	Can Modify State	-
_burn	Internal	Can Modify State	-
transferFrom	Public	Can Modify State	-
safeTransferFrom	Public	Can Modify State	-
ownerOf	Public	-	-
setResolver	External	Can Modify State	onlyPlatformAdmin
nameExpires	Public	-	-
available	Public	-	-
register	External	Can Modify State	-
registerOnly	External	Can Modify State	-
_register	Internal	Can Modify State	live onlyTldController
renew	External	Can Modify State	live onlyTldController
reclaim	External	Can Modify State	live
supportsInterface	Public	-	-
setURI	External	Can Modify State	onlyPlatformAdmin
tokenURI	Public	-	-

RegistrarController			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	-
initialize	External	Can Modify State	initializer
_authorizeUpgrade	Internal	Can Modify State	onlyPlatformAdmin
setTldConfigs	Public	Can Modify State	onlyTldOwner

RegistrarController			
setTldHooks	Public	Can Modify State	onlyTldOwner
setTldPriceOracle	Public	Can Modify State	onlyTldOwner
setMinDomainLength	Public	Can Modify State	onlyTldOwner
setMaxDomainLength	Public	Can Modify State	onlyTldOwner
setMintCap	Public	Can Modify State	onlyTldOwner
setMinRegistrationDuration	Public	Can Modify State	onlyTldOwner
setMinRenewDuration	Public	Can Modify State	onlyTldOwner
setQualificationHook	Public	Can Modify State	onlyTldOwner
setPriceHook	Public	Can Modify State	onlyTldOwner
setPointHook	Public	Can Modify State	onlyTldOwner
setRewardHook	Public	Can Modify State	onlyTldOwner
setRenewPriceHook	Public	Can Modify State	onlyTldOwner
setRenewPointHook	Public	Can Modify State	onlyTldOwner
setRenewRewardHook	Public	Can Modify State	onlyTldOwner
<Receive Ether>	External	Payable	-
recoverFunds	External	Can Modify State	onlyPlatformAdmin
withdraw	Public	Can Modify State	onlyTldOwner
withdrawPlatformFee	Public	Can Modify State	onlyPlatformFeeCollector
getPriceOracle	Public	-	-
rentPriceInUSD	Public	-	-
rentPrice	Public	-	-
priceAfterDiscount	External	-	-
bulkRegister	External	Payable	-

RegistrarController

_bulkRegister	Internal	Can Modify State	-
bulkRenew	External	Payable	-
_distributeFunds	Internal	Can Modify State	-
_renew	Internal	Can Modify State	nonReentrant
_registerWithConfig	Internal	Can Modify State	nonReentrant
_qualify	Private	Can Modify State	-
_newPrice	Private	Can Modify State	-
_deduct	Private	Can Modify State	-
_reward	Private	Can Modify State	-
_newRenewPrice	Private	Can Modify State	-
_deductRenew	Private	Can Modify State	-
_rewardRenew	Private	Can Modify State	-
_registerNode	Private	Can Modify State	-
available	Public	-	-
_setTldName	Internal	Can Modify State	-
_valid	Private	-	-

GiftCardBase

Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	ERC1155 TldAccessable
setURI	External	Can Modify State	onlyPlatformAdmin
uri	Public	-	-
name	Public	-	-

GiftCardBase			
symbol	Public	-	-
register	External	Can Modify State	onlyController whenNotPaused
batchRegister	External	Can Modify State	onlyController whenNotPaused
batchBurn	External	Can Modify State	onlyController whenNotPaused
addController	External	Can Modify State	onlyPlatformAdmin
removeController	External	Can Modify State	onlyPlatformAdmin
pause	External	Can Modify State	onlyPlatformAdmin
unpause	External	Can Modify State	onlyPlatformAdmin
safeBatchTransferFrom	Public	Can Modify State	whenNotPaused

GiftCardController			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
price	Public	-	-
batchRegister	External	Payable	-
batchRedeem	External	Can Modify State	-
setPriceOracle	Public	Can Modify State	onlyPlatformAdmin
withdraw	Public	Can Modify State	onlyTldOwner

GiftCardLedger			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
balanceOf	Public	-	-

GiftCardLedger

redeem	External	Can Modify State	onlyController
deduct	Public	Can Modify State	onlyTldGiftCardController
addTldGiftCardController	External	Can Modify State	onlyTldOwner
removeTldGiftCardController	External	Can Modify State	onlyTldOwner
addController	External	Can Modify State	onlyPlatformAdmin
removeController	External	Can Modify State	onlyPlatformAdmin

GiftCardVoucher

Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
addCustomizedVoucher	External	Can Modify State	onlyTldOwner
totalValue	External	-	-
isValidVoucherIds	External	-	-
getTokenIdTld	External	-	-
isSameTld	Public	-	-

DefaultDiscountHook

Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
calcNewPrice	External	-	-
newPrice	External	Can Modify State	onlyTldController
calcRenewNewPrice	External	-	-
newRenewPrice	External	Can Modify State	onlyTldController
calcDeduction	External	-	-

DefaultDiscountHook

deduct	External	Can Modify State	onlyTldController
calcRenewDeduction	External	-	-
deductRenew	External	Can Modify State	onlyTldController
_calcNewPrice	Private	-	-
_calcPoint	Private	-	-
_calcAuctionExemptation	Private	-	-
_calcGiftCardPoint	Private	-	-
_deductGiftCardPoints	Private	Can Modify State	-
setPreRegiDiscountRateBps	Public	Can Modify State	onlyTldOwner

DefaultQualificationHook

Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
isQualified	Public	-	-
qualify	External	Can Modify State	onlyTldController
_isQualified	Private	-	-
setPublicRegistrationStartTime	Public	Can Modify State	onlyTldOwner onlyBeforePublicRegiStart
setPublicRegistrationPaused	Public	Can Modify State	onlyTldOwner onlyAfterPublicRegiStart
setPreRegistrationState	Public	Can Modify State	onlyTldOwner

PriceOracle

Function Name	Visibility	Mutability	Modifiers

PriceOracle			
<Constructor>	Public	Can Modify State	TldAccessable
initTldPriceModel	External	Can Modify State	onlyTldFactory
_initTldPriceModel	Internal	Can Modify State	-
setTldPriceModel	External	Can Modify State	onlyTldOwner
premium	External	-	-
price	Public	-	-
priceInWei	External	-	-
attoUSDToWei	Public	-	-
weiToAttoUSD	Public	-	-
setUsdOracle	External	Can Modify State	onlyPlatformAdmin
_premium	Internal	-	-
decayedPremium	Public	-	-
addFractionalPremium	Internal	-	-

BaseCreator			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
create	External	Can Modify State	onlyTldFactory

PreRegistrationCreator			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
create	Public	Can Modify State	onlyTldFactory
createAuction	Public	Can Modify State	onlyTldFactory

PreRegistrationCreator

ReferralHub

Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	TldAccessable
calcReward	Public	-	-
calcRenewReward	Public	-	-
reward	External	Payable	onlyTldController
rewardRenew	External	Payable	onlyTldController
_calcReward	Internal	-	-
_reward	Internal	Can Modify State	-
getReferralCommisionFee	Public	-	-
_addNewReferralRecord	Internal	Can Modify State	-
_getReferralCount	Internal	-	-
_getComissionChart	Internal	-	-
getReferralDetails	External	-	-
setComissionChart	External	Can Modify State	onlyTldOwner validLevel
withdraw	External	Can Modify State	nonReentrant

ReverseRegistrar

Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	-
setDefaultResolver	Public	Can Modify State	onlyOwner
claim	Public	Can Modify State	-

ReverseRegistrar			
claimForAddr	Public	Can Modify State	authorised
claimWithResolver	Public	Can Modify State	-
setName	Public	Can Modify State	-
setNameForAddr	Public	Can Modify State	-
setTldName	Public	Can Modify State	-
setTldNameForAddr	Public	Can Modify State	-
node	Public	-	-
sha3HexAddress	Private	-	-
ownsContract	Internal	-	-
setController	Public	Can Modify State	onlyOwner

SidRegistry			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	-
setRecord	External	Can Modify State	-
setSubnodeRecord	External	Can Modify State	-
setOwner	Public	Can Modify State	authorised
setSubnodeOwner	Public	Can Modify State	authorised
setResolver	Public	Can Modify State	authorised
setTTL	Public	Can Modify State	authorised
setApprovalForAll	External	Can Modify State	-
owner	Public	-	-
resolver	Public	-	-

SidRegistry			
ttl	Public	-	-
recordExists	Public	-	-
isApprovedForAll	External	-	-
_setOwner	Internal	Can Modify State	-
_setResolverAndTTL	Internal	Can Modify State	-

4.3 Vulnerability Summary

[N1] [Suggestion] Missing event record

Category: Malicious Event Log Audit

Content

Key Parameter Settings Unrecorded Events .

- contracts/admin/PlatformConfig.sol

The following functions do not log events

`setDefaultMinPlatformFee` , `setDefaultRateBps` , `setPlatformFeeCollector` , `setCustomizedPlatformFee` .

- contracts/admin/SANN.sol

The following functions do not log events

`setTldFactory` , `setPlatformAdmin` , `setMinTldLength` , `setMaxTldLength` , `setTldController` .

- contracts/admin/TldFactory.sol

The following functions do not log events `setDefaultPriceOracle` .

- contracts/giftcard/GiftCardController.sol

The following functions do not log events `setPriceOracle`

Solution

Recording events.

Status

Confirming

[N2] [Suggestion] Existence of unused variables

Category: Others

Content

If a function has some unused variables, you can delete them if you don't need them.

- contracts/hook/DefaultDiscountHook.sol

calcRenewNewPrice unused _extraData.

newPrice unused _extraData.

calcRenewNewPrice unused _extraData.

newRenewPrice unused _extraData.

calcDeduction unused _platformFee,_extraData.

deduct unused _platformFee,_extraData

calcRenewDeduction unuse _platformFee,_extraData.

deductRenew unused _platformFee,_extraData .

_calcNewPrice unused _identifier, _name, _buyer, _duration.

_calcGiftCardPoint unused _name,_duration.

- contracts/admin/TldFactory.sol

_enableQualificationHook unused tldOwner.

- contracts/hook/DefaultQualificationHook.sol

_isQualified unused _identifier, _duration, _extraData.

- contracts/referral/ReferralHub.sol

_calcReward unused _name, _duration, _revenue, _platformFee.

- contracts/proxy/PreRegistrationCreator.sol createAuction unused tldOwner.

Solution

Check that the design expectations are met.

Status

Confirming

[N3] [Suggestion] Redundant code

Category: Others

Content

- contracts/preregistration/PreRegistrationState.sol

`_auctionExtendDuration` is a uint parameter, always greater than 0.So `require( _auctionExtendDuration >= 0, "invalid auctionExtendDuration "invalid auctionExtendDuration" );` is redundant.

```
function _setAuctionConfigs(
        bool _enabled,
        uint _auctionStartTime,
        uint _auctionEndTime,
        uint _auctionExtendDuration,
        uint _auctionRetentionDuration,
        uint _auctionMinRegistrationDuration
    ) internal {
        if (_enabled) {
            require(
                block.timestamp < _auctionStartTime,
                "invalid auctionStartTime"
            );
            require(
                block.timestamp < _auctionEndTime,
                "invalid auctionEndTime"
            );
            require(
                _auctionExtendDuration >= 0,
                "invalid auctionExtendDuration"
            );
            require(
                _auctionStartTime < _auctionEndTime,
                "invalid auctionStartTime"
            );
        }
        auctionEnabled = _enabled;
        auctionStartTime = _auctionStartTime;
        auctionInitialEndTime = _auctionEndTime;
        auctionHardEndTime = auctionInitialEndTime + 1 days;
        auctionExtendDuration = _auctionExtendDuration;
        auctionRetentionDuration = _auctionRetentionDuration;
        auctionMinRegistrationDuration = _auctionMinRegistrationDuration;
        emit SetAuctionConfig(
            identifier,
            _enabled,
            _auctionStartTime,
            _auctionEndTime,
            _auctionExtendDuration,
            _auctionRetentionDuration,
            _auctionMinRegistrationDuration
        );
    }
```

Solution

Can remove useless code.

Status

Confirming

[N4] [Medium] Risk of excessive authority

Category: Authority Control Vulnerability Audit

Content

The roles of `PlatformAdmin` and `TldOwner` are very powerful, if the private key is leaked, it will cause great damage to the project.

- contracts/admin/PlatformConfig.sol

PlatformAdmin can setDefaultMinPlatformFee

PlatformAdmin can setDefaultRateBps

PlatformAdmin can setPlatformFeeCollector

PlatformAdmin can setCustomizedPlatformFee

- contracts/admin/PrepaidPlatformFee.sol

PlatformFeeCollector can withdraw

TldController can deduct

- contracts/admin/SANN.sol

PlatformAdmin can setTldFactory

PlatformAdmin can setPlatformAdmin

PlatformAdmin can setMinTldLength

PlatformAdmin can setMaxTldLength

PlatformAdmin can setTldController

PlatformAdmin can transferNodeOwner

TldFactory can registerTld

TldOwner can setTldOwner

- contracts/admin/TldFactory.sol

PlatformAdmin can createDomainService

PlatformAdmin can setDefaultPriceOracle

contracts/base/Base.sol

PlatformAdmin can setResolver

PlatformAdmin can setURI

- contracts/controller/RegistrarController.sol

PlatformAdmin can recoverFunds

TldOwner can setTldConfigs

TldOwner can setTldHooks

TldOwner can setTldPriceOracle

TldOwner can setMinDomainLength

TldOwner can setMaxDomainLength

TldOwner can setMintCap

TldOwner can setMinRegistrationDuration

TldOwner can setMinRenewDuration

TldOwner can setQualificationHook

TldOwner can setPriceHook

TldOwner can setPointHook

TldOwner can setRewardHook

TldOwner can setRenewPriceHook

TldOwner can setRenewPointHook

TldOwner can setRenewRewardHook

TldOwner can withdraw

PlatformFeeCollector can withdrawPlatformFee

- contracts/giftcard/GiftCardBase.sol

PlatformAdmin can setURI

PlatformAdmin can addController

PlatformAdmin can removeController

PlatformAdmin can pause

PlatformAdmin can unpause

Controller can register

Controller can batchRegister

Controller can batchBurn

- contracts/giftcard/GiftCardController.sol

PlatformAdmin can setPriceOracle

TldOwner can withdraw

- contracts/giftcard/GiftCardLedger.sol

Controller can redeem

TldGiftCardController can deduct

TldOwner can addTldGiftCardController

TldOwner can removeTldGiftCardController

PlatformAdmin can addController

PlatformAdmin can removeController

- contracts/giftcard/GiftCardVoucher.sol

TldOwner can addCustomizedVoucher

- contracts/hook/DefaultDiscountHook.sol

TldController can newPrice

TldController can newRenewPrice

TldController can deduct

TldController can deductRenew

TldOwner can setPreRegiDiscountRateBps

- contracts/hook/DefaultQualificationHook.sol

TldController can qualify

TldOwner can setPublicRegistrationStartTime

TldOwner can setPublicRegistrationPaused

TldOwner can setPreRegistrationState

- contracts/price-oracle/PriceOracle.sol

TldOwner can setTldPriceModel

PlatformAdmin can setUsdOracle

- contracts/proxy/PreRegistrationCreator.sol

TldFactory can create

- contracts/registrar/ReverseRegistrar.sol

TldFactory can create

TldFactory can createAuction

- contracts/registrar/ReverseRegistrar.sol

ReverseRegistrarOwner can setDefaultResolver

ReverseRegistrarOwner can setController

Solution

In the short term, transferring owner ownership to multisig contracts is an effective solution to avoid single-point risk. But in the long run, it is a more reasonable solution to implement a privilege separation strategy and set up multiple privileged roles to manage each privileged function separately. And the authority involving user funds should be managed by the community, and the authority involving emergency contract suspension can be managed by the EOA address. This ensures both a quick response to threats and the safety of user funds.

Status

Confirming

[N5] [Suggestion] Lack of reasonable scope limitations

Category: Others

Content

- contracts/admin/PlatformConfig.sol

`defaultRateBps` can be limited to ensure that it is within a reasonable range.

```
    function setDefaultRateBps(uint256 _rate) external onlyPlatformAdmin {
        defaultRateBps = _rate;
    }
```

- contracts/hook/DefaultDiscountHook.sol

`preRegiDiscountRateBps` can be limited to ensure that it is within a reasonable range.

```
    function setPreRegiDiscountRateBps(
        uint256 rateBps
    ) public onlyTldOwner(identifier) {
        preRegiDiscountRateBps = rateBps;
        emit SetPreRegiDiscountRateBps(identifier, rateBps);
    }
```

Solution

Limit values within reasonable limits.

Status

Confirming

[N6] [Low] Missing zero address validation

Category: Others

Content

- contracts/admin/TldFactory.sol

Missing check for address(0)

```
function setDefaultPriceOracle(
        address _defaultPriceOracle
    ) external onlyPlatformAdmin {
        defaultPriceOracle = _defaultPriceOracle;
    }
```

- contracts/giftcard/GiftCardController.sol

Missing check for address(0)

```
    function setPriceOracle(address _priceOracle) public onlyPlatformAdmin {
        priceOracle = IPriceOracle(_priceOracle);
    }
```

Solution

Check that the address is not zero.

Status

Confirming

[N7] [Low] Missing check for identifier

Category: Others

Content

- contracts/giftcard/GiftCardLedger.sol

It doesn't check if the `identifier` matches the constraints of `onlyTldGiftCardController`, and may not be able to use `deduct` later.

```
function redeem(
    uint256 identifier,
    address account,
    uint256 amount
) external onlyController {
    balances[account][identifier] += amount;
}
```

Solution

Check the identifier to see if the condition is met.

Status

Confirming

[N8] [Suggestion] Preemptive Initialization

Category: Race Conditions Vulnerability

Content

- contracts/controller/RegistrarController.sol

This function has the problem of being preempted.

```
    function initialize(
        ISANN _sann,
        IPlatformConfig _platformConfig,
        IPrepaidPlatformFee _prepaidPlatformFee,
        IPriceOracle _priceOracle,
        IReverseRegistrar _reverseRegistrar
    ) external initializer {
        prepaidPlatformFee = _prepaidPlatformFee;
        defaultPriceOracle = _priceOracle;
        reverseRegistrar = _reverseRegistrar;
        __TldAccessable_init(_sann);
        __TreasuryAccessable_init(_platformConfig);
        __ReentrancyGuard_init();
    }
```

- contracts/admin/SANN.sol

This function has the problem of being preempted.

```
function initialize(
    address _domainRegistry,
    address _platformAdmin
) external initializer {
    chainId = block.chainid;
    currentTldFactory = address(0);
    platformAdmin = _platformAdmin;
    registry = _domainRegistry;
    minTldLength = 3;
    maxTldLength = 5;
}
```

Solution

It is suggested that the initialize operation can be called in the same transaction immediately after the contract is created to avoid being maliciously called by the attacker.

Status

Confirming

5 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002310310001	SlowMist Security Team	2023.10.18 - 2023.10.31	Medium Risk

Summary conclusion: Summary conclusion: The SlowMist security team use a manual and SlowMist team's analysis tool to audit the project, during the audit work we found 1 medium risk, 2 low risk, 5 suggestion vulnerabilities.

6 Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility based on these.

For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.

SLOWMIST

Official Website

www.slowmist.com

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist