Smart Contract Audit Report for Legato

Testers

1. Or Duan
2. Avigdor Sason Cohen
3. ido Shdema

Table of Contents

Management Summary

Legato contacted Sayfer to perform a security audit on their smart contracts.

This report documents the research carried out by Sayfer targeting the selected resources defined under the research scope. Particularly, this report displays the security posture review for Legato smart contracts.

Over the research period, we discovered 8 vulnerabilities in the contracts.

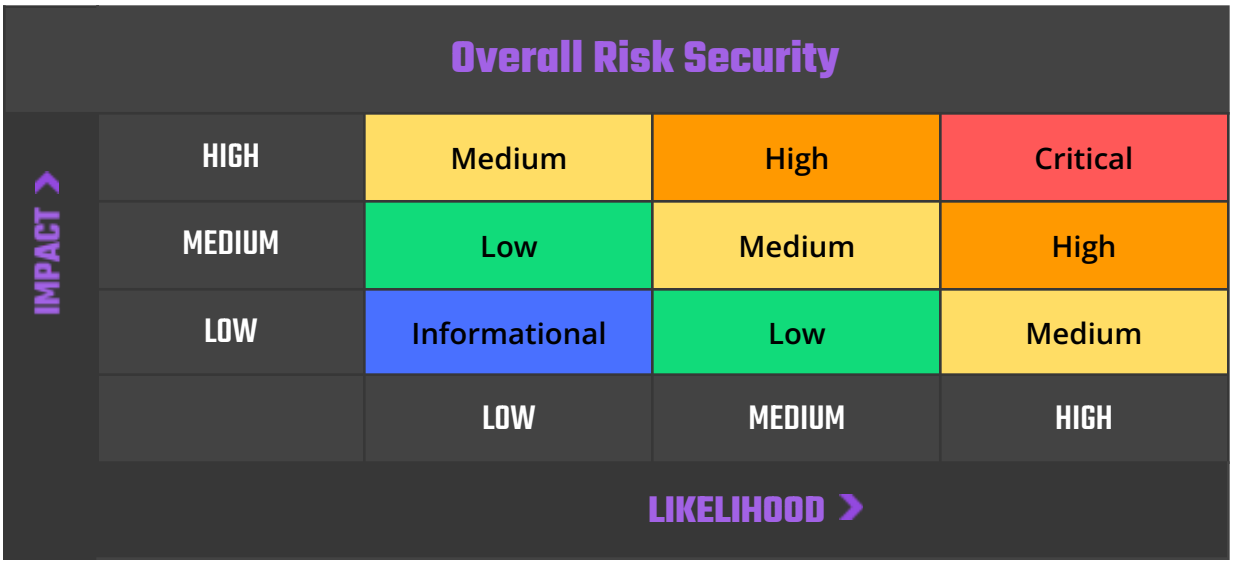
Risk Methodology

At Sayfer, we are committed to delivering the highest quality smart contract audits to our clients. That's why we have implemented a comprehensive risk assessment model to evaluate the severity of our findings and provide our clients with the best possible recommendations for mitigation.

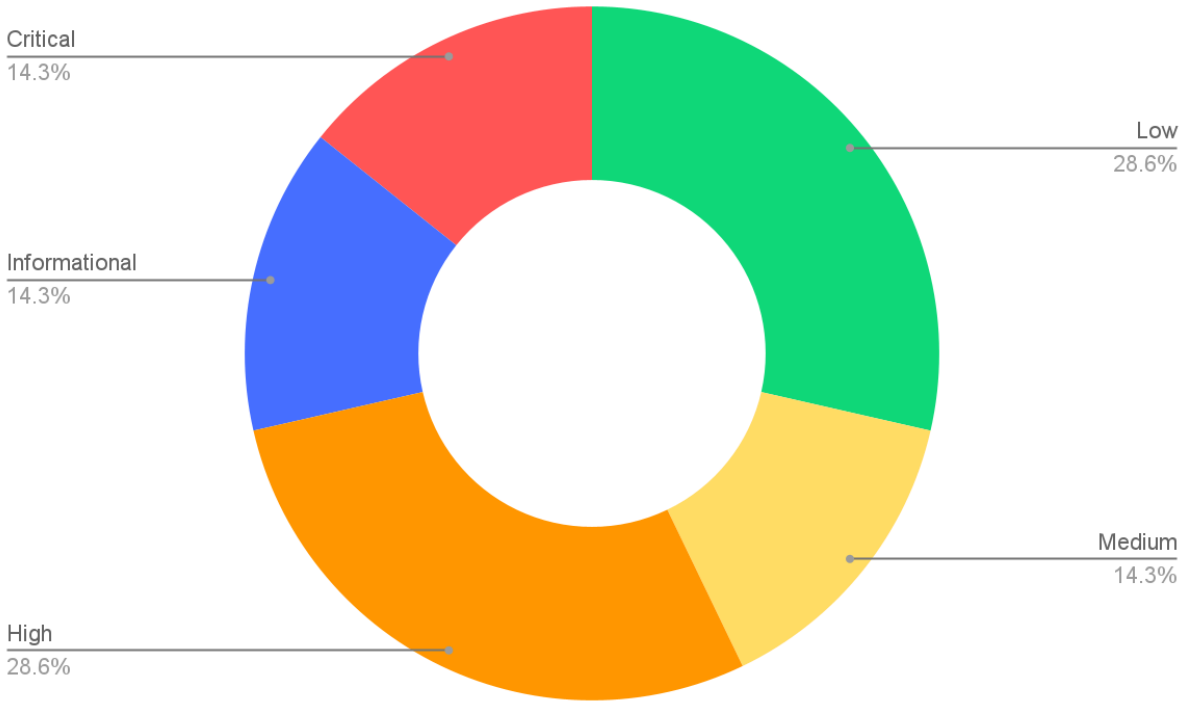
Our risk assessment model is based on two key factors: **IMPACT** and **LIKELIHOOD**. Impact refers to the potential harm that could result from an issue, such as financial loss, reputational damage, or a non-operational system. Likelihood refers to the probability that an issue will occur, taking into account factors such as the complexity of the contract and the number of potential attackers.

By combining these two factors, we can create a comprehensive understanding of the risk posed by a particular issue and provide our clients with a clear and actionable assessment of the severity of the issue. This approach allows us to prioritize our recommendations and ensure that our clients receive the best possible advice on how to protect their smart contracts.

Risk is defined as follows:



Vulnerabilities by Risk



Risk	Low	Medium	High	Critical	Informational
# of issues	3	2	1	0	2

Approach

Introduction

Legato contacted Sayfer to perform a security audit on their smart contracts.

This report documents the research carried out by Sayfer targeting the selected resources defined under the research scope. Particularly, this report displays the security posture review for the aforementioned contracts.

Scope Overview

Together with the client team we defined the following contract as the scope of the project.
Repository: https://github.com/LegatoHQ/legato-infra
Commit hash: bf3c6720fbeefab1e5d34c85373bae872cb6d82a

Our tests were performed in June 2023.

Scope Validation

We began by ensuring that the scope defined to us by the client was technically logical. Deciding what scope is right for a given system is part of the initial discussion.

Threat Model

We defined that the largest current threat to the system is the ability of malicious users to steal funds from the contract.

Security Evaluation

The following test cases were the guideline while auditing the system. This checklist is a modified version of the SCSVS v1.2, with improved grammar, clarity, conciseness, and additional criteria. Where there is a gap in the numbering, an original criterion was removed. Criteria that are marked with an asterisk were added by us.

Architecture, Design and Threat Modeling	Test Name
G1.2	Every introduced design change is preceded by threat modeling.
G1.3	The documentation clearly and precisely defines all trust boundaries in the contract (trusted relations with other contracts and significant data flows).
G1.4	The SCSVS, security requirements or policy is available to all developers and testers.
G1.5	The events for the (state changing/crucial for business) operations are defined.
G1.6	The project includes a mechanism that can temporarily stop sensitive functionalities in case of an attack. This mechanism should not block users' access to their assets (e.g. tokens).
G1.7	The amount of unused cryptocurrencies kept on the contract is controlled and at the minimum acceptable level so as not to become a potential target of an attack.
G1.8	If the fallback function can be called by anyone, it is included in the threat model.
G1.9	Business logic is consistent. Important changes in the logic should be applied in all contracts.
G1.10	Automatic code analysis tools are employed to detect vulnerabilities.
G1.11	The latest major release of Solidity is used.
G1.12	When using an external implementation of a contract, the most recent version is used.
G1.13	When functions are overridden to extend functionality, the super keyword is used to maintain previous functionality.
G1.14	The order of inheritance is carefully specified.
G1.15	There is a component that monitors contract activity using events.
G1.16	The threat model includes whale transactions.
G1.17	The leakage of one private key does not compromise the security of the entire project.

Policies and Procedures	Test Name

G2.2	The system's security is under constant monitoring (e.g. the expected level of funds).
G2.3	There is a policy to track new security vulnerabilities and to update libraries to the latest secure version.
G2.4	The security department can be publicly contacted and that the procedure for handling reported bugs (e.g., thorough bug bounty) is well-defined.
G2.5	The process of adding new components to the system is well defined.
G2.6	The process of major system changes involves threat modeling by an external company.
G2.7	The process of adding and updating components to the system includes a security audit by an external company.
G2.8	In the event of a hack, there's a clear and well known mitigation procedure in place.
G2.9	The procedure in the event of a hack clearly defines which persons are to execute the required actions.
G2.10	The procedure includes alarming other projects about the hack through trusted channels.
G2.11	A private key leak mitigation procedure is defined.

Upgradability	**Test Name**
G2.2	Before upgrading, an emulation is made in a fork of the main network and everything works as expected on the local copy.
G2.3	The upgrade process is executed by a multisig contract where more than one person must approve the operation.
G2.4	Timelocks are used for important operations so that the users have time to observe upcoming changes (please note that removing potential vulnerabilities in this case may be more difficult).
G2.5	*initialize()* can only be called once.
G2.6	*initialize()* can only be called by an authorized role through appropriate modifiers (e.g. *initializer*, *onlyOwner*).
G2.7	The update process is done in a single transaction so that no one can front-run it.
G2.8	Upgradeable contracts have reserved gap on slots to prevent overwriting.
G2.9	The number of reserved (as a gap) slots has been reduced appropriately if new variables have been added.
G2.10	There are no changes in the order in which the contract state variables are declared, nor their types.
G2.11	New values returned by the functions are the same as in previous versions of the contract (e.g. *owner()*, *balanceOf(address)*).
G2.12	The implementation is initialized.
G2.13	The implementation can't be destroyed.

Business Logic	Test Name
G4.2	The contract logic and protocol parameters implementation corresponds to the documentation.
G4.3	The business logic proceeds in a sequential step order and it is not possible to skip steps or to do it in a different order than designed.
G4.4	The contract has correctly enforced business limits.
G4.5	The business logic does not rely on the values retrieved from untrusted contracts (especially when there are multiple calls to the same contract in a single flow).
G4.6	The business logic does not rely on the contract's balance (e.g., *balance == 0*).
G4.7	Sensitive operations do not depend on block data (e.g., *block hash*, *timestamp*).
G4.8	The contract uses mechanisms that mitigate transaction-ordering (front-running) attacks (e.g. pre-commit schemes).
G4.9	The contract does not send funds automatically, but lets users withdraw funds in separate transactions instead.

Access Control	Test Name
G5.2	The principle of the least privilege is upheld. Other contracts should only be able to access functions and data for which they possess specific authorization.
G5.3	New contracts with access to the audited contract adhere to the principle of minimum rights by default. Contracts should have a minimal or no permissions until access to the new features is explicitly granted.
G5.4	The creator of the contract complies with the principle of the least privilege and their rights strictly follow those outlined in the documentation.
G5.5	The contract enforces the access control rules specified in a trusted contract, especially if the dApp client-side access control is present and could be bypassed.
G5.6	Calls to external contracts are only allowed if necessary.
G5.7	Modifier code is clear and simple. The logic should not contain external calls to untrusted contracts.
G5.8	All user and data attributes used by access controls are kept in trusted contracts and cannot be manipulated by other contracts unless specifically authorized.
G5.9	the access controls fail securely, including when a revert occurs.
G5.10	If the input (function parameters) is validated, the positive validation approach (whitelisting) is used where possible.

Communication	Test Name
G6.2	Libraries that are not part of the application (but the smart contract relies on to operate) are identified.

G6.3	Delegate call is not used with untrusted contracts.
G6.4	Third party contracts do not shadow special functions (e.g. revert).
G6.5	The contract does not check whether the address is a contract using *extcodesize* opcode.
G6.6	Re-entrancy attacks are mitigated by blocking recursive calls from other contracts and following the Check-Effects-Interactions pattern. Do not use the *send* function unless it is a must.
G6.7	The result of low-level function calls (e.g. *send*, *delegatecall*, *call*) from other contracts is checked.
G6.8	Contract relies on the data provided by the right sender and does not rely on tx.origin value.

Arithmetic	Test Name
G7.2	The values and math operations are resistant to integer overflows. Use SafeMath library for arithmetic operations before solidity 0.8.*.
G7.3	the unchecked code snippets from Solidity ≥ 0.8.* do not introduce integer under/overflows.
G7.4	Extreme values (e.g. maximum and minimum values of the variable type) are considered and do not change the logic flow of the contract.
G7.5	Non-strict inequality is used for balance equality.
G7.6	Correct orders of magnitude are used in the calculations.
G7.7	In calculations, multiplication is performed before division for accuracy.
G7.8	The contract does not assume fixed-point precision and uses a multiplier or store both the numerator and denominator.

Denial of Service	Test Name
G8.2	The contract does not iterate over unbound loops.
G8.3	Self-destruct functionality is used only if necessary. If it is included in the contract, it should be clearly described in the documentation.
G8.4	The business logic isn't blocked if an actor (e.g. contract, account, oracle) is absent.
G8.5	The business logic does not disincentivize users to use contracts (e.g. the cost of transaction is higher than the profit).
G8.6	Expressions of functions assert or require have a passing variant.
G8.7	If the fallback function is not callable by anyone, it is not blocking contract functionalities.
G8.8	There are no costly operations in a loop.
G8.9	There are no calls to untrusted contracts in a loop.
G8.10	If there is a possibility of suspending the operation of the contract, it is also

	possible to resume it.
G8.11	If whitelists and blacklists are used, they do not interfere with normal operation of the system.
G8.12	There is no DoS caused by overflows and underflows.

Blockchain Data	Test Name
G9.2	Any saved data in contracts is not considered secure or private (even private variables).
G9.3	No confidential data is stored in the blockchain (passwords, personal data, token etc.).
G9.4	Contracts do not use string literals as keys for mappings. Global constants are used instead to prevent Homoglyph attack.
G9.5	Contract does not trivially generate pseudorandom numbers based on the information from blockchain (e.g. seeding with the block number).

Gas Usage and Limitations	Test Name
G10.2	Gas usage is anticipated, defined and has clear limitations that cannot be exceeded. Both code structure and malicious input should not cause gas exhaustion.
G10.3	Function execution and functionality does not depend on hard-coded gas fees (they are bound to vary).

Clarity and Readability	Test Name
G11.2	The logic is clear and modularized in multiple simple contracts and functions.
G11.3	Each contract has a short 1-2 sentence comment that explains its purpose and functionality.
G11.4	Off-the-shelf implementations are used, this is made clear in comment. If these implementations have been modified, the modifications are noted throughout the contract.
G11.5	The inheritance order is taken into account in contracts that use multiple inheritance and shadow functions.
G11.6	Where possible, contracts use existing tested code (e.g. token contracts or mechanisms like *ownable*) instead of implementing their own.
G11.7	Consistent naming patterns are followed throughout the project.
G11.8	Variables have distinctive names.
G11.9	All storage variables are initialized.
G11.10	Functions with specified return type return a value of that type.

G11.11	All functions and variables are used.
G11.12	*require* is used instead of *revert* in *if* statements.
G11.13	The *assert* function is used to test for internal errors and the *require* function is used to ensure a valid condition in input from users and external contracts.
G11.14	Assembly code is only used if necessary.

Test Coverage	Test Name
G12.2	Abuse narratives detailed in the threat model are covered by unit tests.
G12.3	Sensitive functions in verified contracts are covered with tests in the development phase.
G12.4	Implementation of verified contracts has been checked for security vulnerabilities using both static and dynamic analysis.
G12.5	Contract specification has been formally verified.
G12.6	The specification and results of the formal verification is included in the documentation.

Decentralized Finance	Test Name
G14.1	The lender's contract does not assume its balance (used to confirm loan repayment) to be changed only with its own functions.
G14.2	Functions that change lenders' balance and/or lend cryptocurrency are non-re-entrant if the smart contract allows borrowing the main platform's cryptocurrency (e.g. Ethereum). It blocks the attacks that update the borrower's balance during the flash loan execution.
G14.3	Flash loan functions can only call predefined functions on the receiving contract. If it is possible, define a trusted subset of contracts to be called. Usually, the sending (borrowing) contract is the one to be called back.
G14.4	If it includes potentially dangerous operations (e.g. sending back more ETH/tokens than borrowed), the receiver's function that handles borrowed ETH or tokens can be called only by the pool and within a process initiated by the receiving contract's owner or another trusted source (e.g. multisig).
G14.5	Calculations of liquidity pool share are performed with the highest possible precision (e.g. if the contribution is calculated for ETH it should be done with 18 digit precision - for Wei, not Ether). The dividend must be multiplied by the 10 to the power of the number of decimal digits (e.g. dividend * 10^18 / divisor).
G14.6	Rewards cannot be calculated and distributed within the same function call that deposits tokens (it should also be defined as non-re-entrant). This protects from momentary fluctuations in shares.
G14.7	Governance contracts are protected from flash loan attacks. One possible

	mitigation technique is to require the process of depositing governance tokens and proposing a change to be executed in different transactions included in different blocks.
G14.8	When using on-chain oracles, contracts are able to pause operations based on the oracles' result (in case of a compromised oracle).
G14.9	External contracts (even trusted ones) that are allowed to change the attributes of a project contract (e.g. token price) have the following limitations implemented: thresholds for the change (e.g. no more/less than 5%) and a limit of updates (e.g. one update per day).
G14.10	Contract attributes that can be updated by the external contracts (even trusted ones) are monitored (e.g. using events) and an incident response procedure is implemented (e.g. during an ongoing attack).
G14.11	Complex math operations that consist of both multiplication and division operations first perform multiplications and then division.
G14.12	When calculating exchange prices (e.g. ETH to token or vice versa), the numerator and denominator are multiplied by the reserves (see the *getInputPrice* function in the *UniswapExchange* contract).

Audit Findings

Centralized Withdrawal

ID	SAYFER-01
Status	Open
Risk	High
Location	- RegistryV2.sol; withdraw(address, address, uint256)
Business Impact	This kind of centralization could drive away users who fear being rug-pulled.

Description	The withdraw function allows a privileged user to withdraw funds from the registry, creating a situation of dangerous centralization. A single wallet can empty the entire registry in a single transaction.
	
	● withdraw(address _token, address _to, uint256 _amount):
	`function withdraw(address _token, address _to, uint256 _amount) public isInitialized onlyActive onlyAdmin {`
	`  require(_to != address(0), "registryv2 - withdraw to address 0");`
	`  if (_token == address(0)) {`
	`  payable(_to).transfer(_amount); //ether`
	`  } else {`
	`  IERC20(_token).transfer(_to, _amount); //erc20`
	`  }`
	`}`

Mitigation	We recommend documenting the function and detailing its intent: why is the admin even able to withdraw funds without any restriction Conversely, a multisig wallet could be used, transferring the privilege to multiple entities and therefore mitigating the centralization risk.

Custom Implementation of Initializers

ID	SAYFER-02
Status	Open
Risk	Medium
Location	- RegistryV2.sol - BlueprintV2.sol - etc.
Business Impact	Although, as far as we understand, the system is functioning as expected in tests, there are two dangers here: - We believe that new developers may find this confusing as it does not follow known practices in the industry - Solutions like OpenZepplin are used for a reason: they have been proven through time and widespread usage to be secure and functional. On the other hand, there may be issues with this custom implementation that we failed to recognize.
Description	Throughout our assessment, we noticed that many contracts have both initializer functions and constructors. Usually, when implementing initialization using well known solutions like OpenZepplin, constructors are not used. • For instance, here is the initializer of RegistryV2:

```
function initialize(string memory _name, address _ownerWallet,
address _parentRegistry, address _verifyHelper)
    public
    override
{
    require(!initialized, "already initialized!");
    ledgerName = _name;
    parentRegistry = IRootRegistry(_parentRegistry);
    verifyHelper = _verifyHelper;
    ownerWallet = _ownerWallet;

    _grantRole(DEFAULT_ADMIN_ROLE, _parentRegistry);
    _grantRole(DEFAULT_ADMIN_ROLE, _ownerWallet);
    _grantRole(PAUSER_ROLE, _ownerWallet);
    initialized = true;
```

```
    storeStatus = StoreStatus.ACTIVE;
}
```

This is seemingly redundant, because the constructor function, which already calls *initialize*, can only be run once:

- RegistryV2.sol; constructor(string, address, address, address):

```
constructor(string memory _name, address _ownerWallet, address
_parentRegistry, address _verifyHelper) {
    initialize(_name, _ownerWallet, _parentRegistry,
_verifyHelper);
}
```

However, we checked with the Legato team and it seems that they choose to implement it like this since the usage of constructors streamlines their testing process.

Mitigation

Our recommendation is to switch to OpenZepplin. This can be done by implementing the OpenZepplin's Initializable contract

- To give an example, for RegistryV2, it would look like this:

```
import
"lib/openzeppelin-contracts/contracts/access/Initializable.sol
";


contract RegistryV2 is IRegistryV2, AccessControl,
IERC721Receiver, Pausable, Initializable {

...

    function initialize(string memory _name, address
_ownerWallet, address _parentRegistry, address _verifyHelper)
        public initializer
    {
        RegistryV2.initialize()

        ledgerName = _name;
        parentRegistry = IRootRegistry(_parentRegistry);
        verifyHelper = _verifyHelper;
```

```
        ownerWallet = _ownerWallet;

        _grantRole(DEFAULT_ADMIN_ROLE, _parentRegistry);
        _grantRole(DEFAULT_ADMIN_ROLE, _ownerWallet);
        _grantRole(PAUSER_ROLE, _ownerWallet);
        storeStatus = StoreStatus.ACTIVE;
    }

...

}
```

Otherwise, if you intend to keep the custom system, we recommend that you leave comments documentation of why you are using it, and what is its purpose, to avoid confusing readers.

Lack of Input Validation

ID	SAYFER-03
Status	Open
Risk	Medium
Location	- RegistryV2.sol; attach(address, address, address, address, address)
Business Impact	Wrong or null addresses where the code expects a valid address can cause unpredictable behavior.

Description	The function *attach* in RegistryV2 receives five different addresses as arguments, but doesn't check if they are not null, identical, or otherwise invalid.
	
	• attach(address, address, address, address, address)
	`function attach(`
	`  address _feeDistributor,`
	`  address _tokenDistributor,`
	`  address _licenseContract,`
	`  address _licenseRegistry,`
	`  address _collectibleReg`
	`) external override isInitialized onlyAdmin {`
	`  feeDistributor = _feeDistributor;`
	`  tokenDistributor = _tokenDistributor;`
	`  licenseRegistry = _licenseRegistry;`
	`  licenseContract = _licenseContract;`
	`  collectibleRegistry = _collectibleReg;`
	`}`

Mitigation	We recommend implementing proper input validation whenever you receive addresses from external sources.

Inefficient Access Control

ID	SAYFER-04
Status	Open
Risk	Low
Location	- RegistryV2.sol; setName(string) - RegistryV2.sol; optOutofLicense(uint256, uint256)
Business Impact	Future versions might not match the code inconsistency which will cause access control vulnerabilities.
Description	The two functions listed require that *msg.sender* has the role admin, however, there is already a modifier that does exactly that. ● setName(string): `function setName(string memory _name) external override { require(hasRole(DEFAULT_ADMIN_ROLE, msg.sender), "must have admin role"); // Replace this require statement with a modifier. ledgerName = _name; }`
Mitigation	The provided example should look like this: `function setName(string memory _name) external override onlyRole(DEFAULT_ADMIN_ROLE) { ledgerName = _name; }`

Inconsistent Usage of Modifiers

ID	SAYFER-05
Status	Open
Risk	Low
Location	- RegistryV2.sol; pause() - RegistryV2.sol; unpause()
Business Impact	Inconsistent coding practices can induce confusion in readers and reduce maintainability and readability.

Description	The two functions listed require that *msg.sender* has the role admin, however, there is already a modifier that does exactly that.
	
	● pause(), notice how the function uses the modifier onlyActive:
	`function pause() public override onlyRole(PAUSER_ROLE) onlyActive { _pause(); storeStatus = StoreStatus.PAUSED; emit StatusUpdated(StoreStatus.PAUSED); }`
	● unpause(), no modifier is used, and isInitialized appears to be redundant, it is not clear how can the function be called if the contract was not yet initialized, yet the design seems wrong.
	`function unpause() public override isInitialized onlyRole(PAUSER_ROLE) { if (storeStatus != StoreStatus.PAUSED) { revert WrongBaseStatus(storeStatus); } _unpause(); storeStatus = StoreStatus.ACTIVE; emit StatusUpdated(StoreStatus.ACTIVE); }`

Mitigation	- Remove isInitialized from *unpause()*. - Introduce a new modifier *onlyPaused* and use it to replace the if statement at the beginning of the function.

Use SafeERC20

ID	SAYFER-06
Status	Open
Risk	Low
Location	- FeeDistributor.sol; 145-147; claimByID(uint256) - FeeDistributor.sol; 169, 184, 186; payStore(FeeInfo) - FeeDistributor.sol; 210, 212; pay(FeeInfo) - FeeDistributor.sol; 288; withdrawFees(address, address, uint256)
Business Impact	SafeERC20 is designed to safeguard from improperly implemented ERC20 tokens that don't revert on failiure. The danger is that if that return value is used in the code, and the token returns nothing, the contract will simply take whatever it could find in memory, essentially gibberish. You could read more about this in this article.
Description	During our assessment we found multiple instances of multiple locations across the code, particularly in *FeeDistributor.sol*. It is considered best practice to employ safer implementations.

Mitigation	Use OpenZepplin's SafeERC20, as detailed in here.
	
	The switch from normal ERC20 to SafeERC20 is extremely simple, with the exception of one function: *approve*.
	
	safeApprove suffers issues similar to *approve*, namely, that it can cause a race condition where someone may use both the old and the new allowance by unfortunate transaction ordering. OpenZepplin therefore deprecated *safeApprove* and recommends using *safeIncreaseAllowance* and *safeDecreaseAllowance* where possible.
	
	If this is not possible, the recommended solution is to first reduce the spender's allowance to 0 and set the desired value afterwards, like this:
	`token.safeApprove(0);`
	`token.safeApprove(_amount);`

Functions Fail to Emit Events

ID	SAYFER-07
Status	Open
Risk	Informational
Location	- RegistryV2.sol; setName(string) - RegistryV2.sol; optOutofLicense(uint256, uint256) - BlueprintV2.sol; bindToken(address) - BlueprintV2.sol; addCollectible(address)
Business Impact	Events help off-chain listeners to track the state of the contract when emitted with meaningful data
Description	Certain functions across the code, like the ones listed above, perform important functionality, but fail to emit events, violating best practices. • BlueprintV2.sol; bindToken(address): `function bindToken(address token) public isInitialized onlyRole(BINDER_ROLE) { require(token != address(0), "cannot add address 0 token"); tokens.push(token); // Consider emitting an event here. }`
Mitigation	Consider adding events for important functions.

Dead Code

ID	SAYFER-08
Status	Open
Risk	Informational
Location	Codebase-wide
Business Impact	While there is no direct business impact, such useless code simply reduces maintainability and readability.

Description	Throughout the codebase, we found multiple instances of dead code: for debugging or otherwise. For instance, commented code or *console.log* calls. The following is just one example.
	
	• RegistryV2.sol; mintIP(BlueprintMintingParams):
	`function mintIP(BlueprintMintingParams memory _params)`
	`external`
	`override`
	`isInitialized`
	`onlyAdmin`
	`onlyActive`
	`returns (address)`
	`{`
	`console.log("in mint song"); // Remove this.`
	`...`
	`}`

Mitigation	Review your code and remove commented code or *console.log*s.