

# CMTAT - Audit-20210910

## Introduction

This document concerned the audit report [ABDK-CMTAT-audit-20210910.pdf](#) which was made on the project [CMTAT](#).

The audited version is that of commit [cd3af7](#)

## Vocabulary

Header	Description		
Id	Id of the concerned CVF		
Severity	Same notation that in the report Color :		
	Minor	Moderate	Major
Object	The concerned object [Functions, variables, event name, etc..]		
Decision	Which decision has been taken and why		
Status	[Fixed] => CVF has been fixed [In progress] => CVF is being fixed (pull request / issue) [Open] => CVF is NOT fixed [No longer relevant] => CVF is no longer relevant, e.g., because the problematic functionality was removed. [Closed] => A decision to not fix the CVF has been taken		

	Fixed	Partially fixed	Open	No longer relevant	Closed
Commit / pull request fix	The concerned commit / pull request on github which fix the CVF				
Remark	Any other relevant information, by example suggestions to fix the CVF.				

## Summary

ID	Severity	Module	Object [Functions, variables, event name, etc..]	Description (evt recommendation)	Decision	Status	Commit / pull request fix	Remark
1	Minor	SnapshotModule.sol All modules are concerned	pragma solidity	Solidity version		Opened		See <a href="#">issues/68</a>
2	Minor	SnapshotModule.sol	-	The version of the imported library should be provided.	The OpenZeppelin version is indicated in the file USAGE.md	Fixed	<a href="#">Pull/98/Commit</a>	
3	Minor	SnapshotModule.sol	-	Provide a short function description and parameter meaning in the comments preceding the function.		Opened		

4	Minor	SnapshotModule.sol	SNAPSHOTER_ROLE	The word “snaphoter” (12K results in Google) sounds odd.	The variable is renamed in snaphooter	Fixed	<a href="#">pull/13 Commit</a>	
5	Minor	SnapshotModule.sol	_currentSnapshot	This variable is not initialized.	explicitly initializing to 0 Fixed	Fixed	<a href="#">pull/14 Commit</a>	The commit fix broke the proxy construction. <a href="#">Commit fix</a>
6	Moderate	SnapshotModule.sol	_scheduledSnapshots	Using an unordered list of scheduled snapshots and removing already created snapshots from it is suboptimal and have several important drawbacks [...]		Opened		
7	Minor	SnapshotModule.sol	scheduleSnapshot	Function scheduleSnapshot always returns its argument.	No return value	Opened	<a href="#">Pull/76 Commit</a>	
8	Minor	SnapshotModule.sol	_rescheduleSnapshot	Here two passes over the array are made while just one suffices.		Opened		
9	Minor	SnapshotModule.sol	_rescheduleSnapshot	This function always returns its second argument which is clearly redundant.	No return value	Fixed	<a href="#">Pull/76 Commit</a>	
10	Minor	SnapshotModule.sol	_unscheduleSnapshot	function always returns its argument which is clearly redundant	No return value	Fixed	<a href="#">Pull/76 Commit</a>	
11	Minor	SnapshotModule.sol	getNextSnapshots()	This method returns also uncleared snapshots from the past.	-	Opened		

12	Minor	SnapshotModule.sol	SnapshotTotalSupply snapshotTotalSupply	Is it desired behaviour that the current balance is returned for an invalid snapshot time?	-	Opened		
13	Moderate	SnapshotModule.sol	_setCurrentSnapshot	This call reads the entire snapshot array, which is a significant overhead over each transfer.	-	Opened		
14	Minor	SnapshotModule.sol	_beforeTokenTransfer	The most often used branch is the last one.	refactoring order of conditions as indicated in the audit report	Fixed	<a href="#">pull/16</a> <a href="#">Commit</a>	
15	Minor	SnapshotModule.sol	_valueAt	Semantics of returned values is unclear		Opened		
16	Minor	SnapshotModule.sol	_getCurrentSnapshot	This function is redundant as it just returns the value of a storage variable.		Opened		
17	Minor	SnapshotModule.sol	Several functions (see report)	These loops do linear searches through the array whose length is unlimited. This makes the contract vulnerable to DoS attacks by scheduling a large number of snapshots.		Opened		
18	Minor	SnapshotModule.sol	_clearPastScheduled()	The “_scheduledSnapshots.length” value is read on every iteration.		Opened		

19	Minor	SnapshotModule.sol	_clearPastScheduled()	The element to be moved to this position will be once again read from storage at the next iteration		Opened		
20	Minor	SnapshotModule.sol	_removeScheduledItem	This line executes even if index is the last element.		Opened		
21	Minor	SnapshotModule.sol	event RuleEngineSet	The parameter type should be "IRuleEngine".		Opened		
22	Minor	ValidationModule.sol	IRule Engine public rule Engine	This module should use "IRule" instead of "IRuleEngine" as it doesn't need to know that the rule used is actually a composition of several nested rules.		Opened		
23	Minor	ValidationModule.sol	IRule Engine public ruleEngine	The module doesn't allow changing the rule engine after the deployment.	The module ValidationModule implements now a function setRuleEngine. This function was moved from CMTAT.sol to the concerned module	Fixed	<a href="#">pull/88 Commit</a>	
24	Minor	ValidationModule.sol	_validateTransfer	This will revert in case the rule engine is not set.		Opened		
25	Minor	ValidationModule.sol	_messageForTransferRestrict	This will revert in case the rule engine is not set.		Opened		

			ction					
26	Minor	ValidationModule.sol	_detectTransferRestriction	This will revert in case the rule engine is not set.		Opened		
27	Minor	CMTAT.sol	TRANSFER_OK	Defining restriction code constants in several places is error-prone.	Define an enum in CMTAT.sol for the restriction code	Partially fixed	<a href="#">Pull/78 Commit</a>	Messages are still defined in each file. Other concerned CTF : CTF-48, CTF-55
28	Moderate	CMTAT.sol	__CMTAT_init	There should be a call to the “__Validation_init_unchained” function somewhere after this call.		Opened		
29	Minor	CMTAT.sol	__CMTAT_init	There should be a call to the “__ERC165_init_unchained” function before this call.	Proposed changes have been implemented	Fixed	<a href="#">Pull/105 Commit</a>	
30	Minor	CMTAT.sol	__CMTAT_init	This should be done before the “__Base_init_unchained” call as Base module inherits from ERC20 module.	Proposed changes have been implemented  Later, the ERC20 functions have been moved from BaseModule to ERC20BaseModuleFixed	Fixed	<a href="#">Pull/105 Commit</a>	

31	Minor	CMTAT.sol	__CMTAT_init	There should be a call to the “__ERC2771Context_init_unchained” function before this call.	No more relevant because __ERC2771Context_init_unchained” do not exist anymore in the recent version of OZ	No longer relevant		
32	Minor	CMTAT.sol	mint	This event should be emitted inside the “_mint” function.	_mint is a function from OpenZeppelin library. It is not possible to modify it directly. We can override it but it is a bit overkill	Closed		
33	Minor	CMTAT.sol	BurnFrom (replaced by forceBurn in the version 2.1)	This would emit the “Approval” event (which is not desired) but will not emit the “Spend” event (which is actually desired).	No more relevant, the concerned code was removed by replacing the function burnFrom by forceBurn	No longer relevant		
34	Minor	CMTAT.sol	BurnFrom (replaced by forceBurn in the version 2.1)	This event should be emitted inside the “_burn” function.	_burn is a function from OpenZeppelin library. It is not possible to modify it directly. We can override it but it is a bit overkill	Closed		
35	Minor	CMTAT.sol	Several functions (see report)	With multiple inheritance, it is unclear what base contract is referred as “super” here.	The parent module / base contract is explicitly indicated.	Fixed	<a href="#">Pull/92 Commit</a> <a href="#">pull/93 Commit</a>	

36	Minor	CMTAT.sol	DetectTransferRestriction messageForTransferRestriction	This logic should be moved to the "PauseModule" contract.	The ValidationModule defines the different code of rejection, it is better to keep all the validation logic in the same module.	Closed		
37	Minor	CMTAT.sol	detectTransferRestriction	Should be "}" else" for readability.	Proposed changes have been implemented	Fixed	<a href="#">Pull/17</a> <a href="#">Commit</a>	
38	Minor	CMTAT.sol	DetectTransferRestriction messageForTransferRestriction	This logic should be moved to the "EnforcementModule" contract.	The ValidationModule defines the different code of rejection, it is better to keep all the validation logic in the same module.	Closed		
39	Minor	CMTAT.sol		This logic should be moved to the "ValidationModule".	Proposed changes have been implemented	Fixed	<a href="#">Commit</a> <a href="#">pull/89</a>	
40	Minor	CMTAT.sol	setTokenId setTerms <del>setTrustedForwarder</del>	These functions should log some event.  The function setTrustedForwarder was removed from the code.	Define events setTokenId & setTerms	Fixed	<a href="#">Pull/80</a> <a href="#">Commit</a>	
41	Minor	CMTAT.sol	kill	Due to various misuse cases, it is best practice to use selfdestruct only when multiple short-lived contracts	The function kill is a legal requirement, it can not be removed. Protections were added :	Closed	<a href="#">pull/102</a>	



				are created	- If the CMTAT is deployed with a proxy, the function kill can only be triggered through the proxy - The function is protected by an access control			
42	Minor	CMTAT.sol	_beforeToken Transfer	These checks should be the first to save gas.	Proposed changes have been implemented	Fixed	<a href="#">Pull/18 Commit</a>	
43	Minor	CMTAT.sol	_beforeToken Transfer	This check should be done in the "PauseModule" smart contract.		Opened		
44	Minor	CMTAT.sol	_beforeToken Transfer	This check should be done in the "EnforcementModule" smart contract.		Opened		
45	Minor	CMTAT.sol	_beforeToken Transfer	This code should be moved to the "ValidationModule" smart contract.	Move the concerned code inside the ValidationModule	Fixed	<a href="#">Commit pull/89</a>	
46	Minor	PauseModule.sol	-	The version of the imported library (OZ) should be provided.	The OpenZeppelin version is indicated in the file USAGE.md	Fixed	<a href="#">Pull/98/Commit</a>	
47	Minor	PauseModule.sol	-	This contract should defines the "__Pause_init" and "__Pause_init_unchained" functions.	Define the functions PauseModule_init & PauseModule_init_unchained	Fixed	<a href="#">Pull/104 Commit</a>	

48	Minor	PauseModule.sol	TRANSFER_REJECTED_PAUSED	Defining constants for different transfer rejection reasons in different contracts is error-prone	Define an enum in CMTAT.sol	Fixed	<a href="#">Pull/78 Commit</a>	
49	Minor	AuthorizationModule.sol	-	The version of the imported library (OZ) should be provided.	The OpenZeppelin version is indicated in the file USAGE.md	Fixed	<a href="#">Pull/98/ Commit</a>	
50	Minor	AuthorizationModule.sol	-	It is a good practice to put a comment into an empty block to explain why it is empty.	The block is no longer empty.	No longer relevant		
51	Minor	AuthorizationModule.sol	-	This contract should define the “__Authorization_init” and “__Authorization_init_unchained” functions.	Define the functions Authorization_init & Authorization_init_unchained	Fixed	<a href="#">Pull/104 Commit</a>	
52	Minor	MintModule.sol	-	This module doesn't actually implement minting functionality.	Move the mint functionality inside the MintModule	Fixed	<a href="#">pull/88 Commit</a>	
53	Minor	EnforcementModule.sol		The version of the imported library (OZ) should be provided.	The OpenZeppelin version is indicated in the file USAGE.md	Fixed	<a href="#">Pull/98/ Commit</a>	
54	Minor	EnforcementModule.sol	Freeze Unfreeze	These events should probably also have the “reason” parameter.		Opened		
55	Minor	EnforcementModule.sol	TRANSFER_REJECTED_F	Defining constants for different transfer rejection reasons in different contracts	Define an enum in CMTAT.sol	Fixed	<a href="#">Pull/78 Commit</a>	

			ROZEN	is error-prone.				
56	Moderate	EnforcementModule.sol	TEXT_TRANSFER_REJECTED_FROZEN	The message is exactly the same as in the "PauseModule" contract. Also, the message is misleading.	The text message has been changed	Fixed	<a href="#">Pull/79</a> <a href="#">Commit</a>	
57	Minor	MetaTxModule.sol	-	The version of the imported library (OZ) should be provided.	The OpenZeppelin version is indicated in the file USAGE.md	Fixed	<a href="#">Pull/98/</a> <a href="#">Commit</a>	
58	Minor	MetaTxModule.sol	__MetaTx_init	This code relies on how the base contract is implemented.	No more relevant because __ERC2771Context_init_unchained" do not exist anymore in the recent version of OZ	No longer relevant		
59	Major	MetaTxModule.sol	__MetaTx_init_unchained	An unchained initializer is not supposed to call the base contract initializer.	The problematic function call was removed.	Fixed	<a href="#">Commit</a>	
60	Minor	BurnModule.sol	-	The version of the imported library (OZ) should be provided.	The OpenZeppelin version is indicated in the file USAGE.md	Fixed	<a href="#">Pull/98/</a> <a href="#">Commit</a>	
61	Minor	BurnModule.sol	-	a) This module doesn't actually implement burning. b) Also, it inherits from the "Initializable" interface but doesn't have any initializer functions	- Move the burn functionality inside the BurnModule - Add initialize functions	Fixed	a) <a href="#">pull/88</a> <a href="#">Commit</a>  b) <a href="#">pull/104</a> <a href="#">Commit</a>	

62	Minor	BaseModule.sol	-	The version of the imported library (OZ) should be provided.	The OpenZeppelin version is indicated in the file USAGE.md	Fixed	<a href="#">Pull/98/Commit</a>	
63	Minor	BaseModule.sol	-	This requirement is not present in the module documentation	The requirement was added to the documentation in base.md	Fixed	<a href="#">Pull/19/Commit</a>	
64	Major	BaseModule.sol	transferFrom	The returned value is ignored.	Proposed changes have been implemented	Fixed	<a href="#">Commit</a>	
65	Major	BaseModule.sol	approve	It would be better to call “super.approve” here. The current code relies on the knowledge of how the base contract is implemented.	Proposed changes have been implemented	Fixed	<a href="#">Commit</a>	
66	Minor	IRuleEngine.sol	-	It is common practice to provide a short function description and parameter meaning in the comments preceding the function.	Proposed changes have been implemented	Fixed	<a href="#">Pull/74/Commit</a>	
67	Minor	IRuleEngine.sol	-	This interface is redundant. It basically defines a composite rule, i.e. a rule composed from other rules, but for those tokens that use	Not fixed, it is no real necessary to fix this CWF, it is clearer to separate IRuleEngine and IRule. Thus, we	Closed		

				such composite rule, it's composite nature doesn't not make any difference and is basically an implementation details.	have a clear separation between the engine and the rules.			
68	Minor	IRuleEngine.sol	setRules	Setting all rules at once effectively limits the maximum number of rules, as size of a transaction is limited by block gas limit.		Opened		not fixed, the remove functionality makes the code more complicated.
69	Minor	IRuleEngine.sol	ValidateTransfer detectTransferRestriction messageForTransferRestriction	These functions are very similar to the functions defined in the "IRule" interface.	Create two interfaces IERC1404 & IERC1404Wrapper (initially called IERC1404Common)	Fixed	<a href="#">Pull/74</a> <a href="#">Commit-1</a> <a href="#">Commit-2</a>	
70	Minor	IRule.sol	-	It is common practice to provide a short function description and parameter meaning in the comments preceding the function.	Proposed changes have been implemented	Fixed	<a href="#">pull/74</a> <a href="#">Commit</a>	
71	Minor	IRule.sol	IRule	The interface name is too generic. The interface is all about transfers, consider reflecting this in the name.		Opened		
72	Minor	IRule.sol	detectTransfer	The semantics of these	Add a short description +	Fixed	<a href="#">pull/74</a>	

			Restriction canReturnTransferRestrictionCode messageForTransferRestriction	functions is unclear from their signatures.	create interface IERC1404		<a href="#">Commit</a>	
73	Minor	IRule.sol	DetectTransferRestriction canReturnTransferRestrictionCode messageForTransferRestriction	Types narrower than 256 bits don't save gas when used with function arguments or return values, however they limit the range of possible values.	No change The original goal was to be compliant with EIP-1404: <a href="#">ethereum/EIPs#1404</a> and restrictionCode is uint8	Closed	See <a href="#">pull/70</a>	Remark on the save gas part The parameter argument is linked with variable stored in storage and in storage use uint8 rather than 256 can save gas