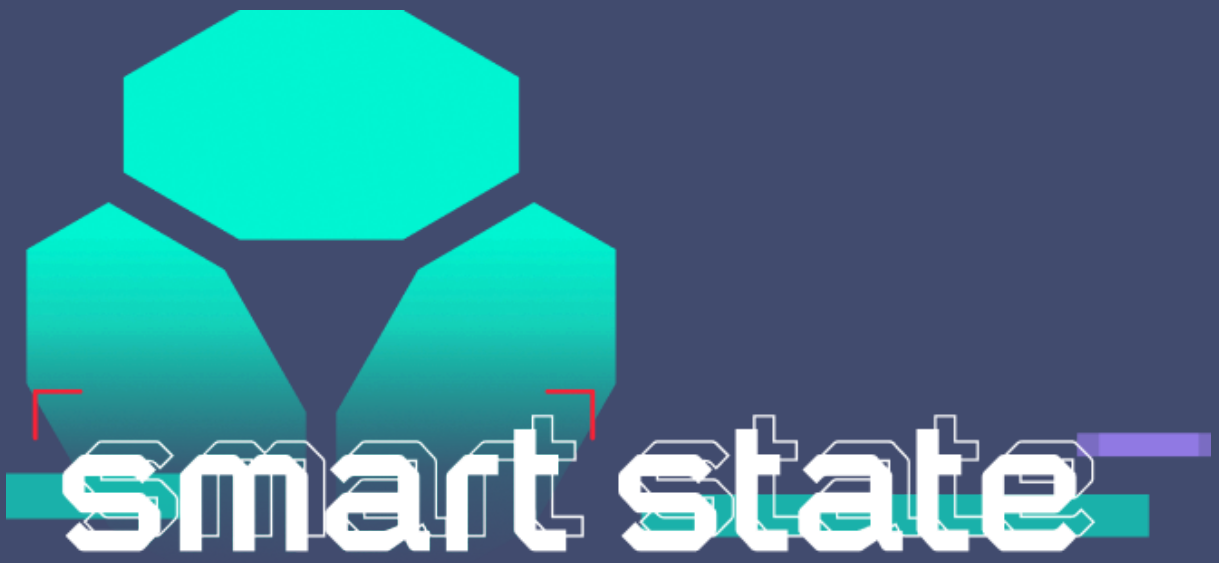

EYWA

CLP
Smart Contract Audit Interim Report

Ver. 1.1
27/03/2024

Table of Contents:

Vulnerabilities found by type:

INFO	0
WARNING	1
WARNING	0
TOTAL:	1

1. AddressBook

Contract methods analysis:

bridge() returns(address)
Vulnerabilities not detected

setPortal(AddressBook.Record[]) returns()
Vulnerabilities not detected

setSynthesis(AddressBook.Record[]) returns()
Vulnerabilities not detected

setRouter(AddressBook.Record[]) returns()
Vulnerabilities not detected

`setTreasury(address) returns()`
Vulnerabilities not detected

`setGateKeeper(address) returns()`
Vulnerabilities not detected

`setWhitelist(address) returns()`
Vulnerabilities not detected

`_setRecords(mapping(uint64 => address), AddressBook.Record[],AddressBook.RecordTypes) returns()`
Vulnerabilities not detected

`_emitEvent(address,uint64,AddressBook.RecordTypes) returns()`
Vulnerabilities not detected

`_checkAddress(address) returns()`
Vulnerabilities not detected

2. BaseRouter

Contract methods analysis:

`constructor(address) returns()`
Vulnerabilities not detected

`nonces(address) returns(uint256)`
Vulnerabilities not detected

`registerComplexOp(BaseRouter.ComplexOp[]) returns()`
Vulnerabilities not detected

`setAddressBook(address) returns()`
Vulnerabilities not detected

`pause() returns()`
Vulnerabilities not detected

`unpause() returns()`
Vulnerabilities not detected

`_start(string[],bytes[],IRouterParams.Invoice) returns()`
Vulnerabilities not detected

`_resume(bytes32,uint8,string[],bytes[]) returns()`
Vulnerabilities not detected

`_execute(uint256,string[],bytes[]) returns(bytes32,uint64,BaseRouter.ExecutionResult,uint8)`
Vulnerabilities not detected

`_getAndUpdateNonce(address) returns(uint256)`
Vulnerabilities not detected

`_checkSignature(address,bytes32,bytes, IRouterParams.Invoice) returns(address)`
Vulnerabilities not detected

`_getRawData(string[],bytes[]) returns(bytes32,bytes)`
Vulnerabilities not detected

`_getRequestId(address,uint64) returns(bytes32)`
Vulnerabilities not detected

`_proceedFees(uint256,address) returns()`
Vulnerabilities not detected

`_executeOp(bool,bytes32,bytes32,bytes, BaseRouter.MaskedParams) returns(uint64,bytes,BaseRouter.MaskedParams, BaseRouter.ExecutionResult)`
Vulnerabilities not detected

3. RouterV2

Contract methods analysis:

`constructor(address) returns()`
Vulnerabilities not detected

`receive() returns()`
Vulnerabilities not detected

`receiveValidatedData(bytes4,address,uint64) returns(bool)`
Vulnerabilities not detected

`start(string[],bytes[],IRouterParams.Invoice) returns()`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, public

`resume(bytes32,uint8,string[],bytes[]) returns()`
Vulnerabilities not detected

`_executeOp(bool,bytes32,bytes32,bytes, BaseRouter.MaskedParams) returns(uint64,bytes,BaseRouter.MaskedParams, BaseRouter.ExecutionResult)`
Vulnerabilities not detected

`_lock(IRouterParams.SynthParams) returns()`
Vulnerabilities not detected

`_unlock(IRouterParams.SynthParams) returns(uint256)`
Vulnerabilities not detected

`_emergencyUnlock(IRouterParams.SynthParams) returns(uint256)`
Vulnerabilities not detected

`_mint(IRouterParams.SynthParams) returns(uint256)`
Vulnerabilities not detected

`_emergencyMint(IRouterParams.SynthParams) returns(uint256)`
Vulnerabilities not detected

`_wrap(IRouterParams.WrapParams) returns(uint256)`
Vulnerabilities not detected

`_unwrap(IRouterParams.WrapParams) returns(uint256)`
Vulnerabilities not detected

`_proceedFees(uint256,address) returns()`
Vulnerabilities not detected

`_checkMaskedParams(uint256,address,address,BaseRouter.MaskedParams) returns(uint256,address,address)`
Vulnerabilities not detected

`_checkTo(address,address,uint64,bytes32) returns(address)`
Vulnerabilities not detected

4. SynthesisV2

Contract methods analysis:

`constructor(address) returns()`
Vulnerabilities not detected

`setAddressBook(address) returns()`
Vulnerabilities not detected

`setCap(address,uint256) returns()`
Vulnerabilities not detected

`getSynth(uint64,address) returns(address)`
Vulnerabilities not detected

`mint(address,uint256,address,address,uint64) returns(uint256)`
Vulnerabilities not detected

`emergencyMint(address,uint256,address,address) returns(uint256)`
Vulnerabilities not detected

`burn(address,uint256,address,address,uint64) returns()`
Vulnerabilities not detected

`setSynths(address[]) returns()`
Vulnerabilities not detected

`_setSynth(address) returns()`
Vulnerabilities not detected

5. ThirdPartySynthAdapter

Contract methods analysis:

`constructor(address,address,uint64,string,uint8) returns()`
Vulnerabilities not detected

`setCap(uint256) returns()`
Vulnerabilities not detected

`mint(address,uint256) returns()`
Vulnerabilities not detected

`burn(address,uint256) returns()`
Vulnerabilities not detected

6. UnifiedRouterV2

Contract methods analysis:

`constructor(address) returns()`
Vulnerabilities not detected

`setPoolAdapter(address,address) returns()`
Vulnerabilities not detected

`_executeOp(bool,bytes32,bytes32,bytes, BaseRouter.MaskedParams) returns(uint64,bytes,BaseRouter.MaskedParams, BaseRouter.ExecutionResult)`
Vulnerabilities not detected

`_checkTo(address,address,uint64,bytes32) returns(address)`
Vulnerabilities not detected

`_getPoolAdapter(address) returns(address)`
Vulnerabilities not detected

`_transferToAdapter(address,address,address,uint256) returns()`
Vulnerabilities not detected

7. adapters/crypto1/PoolAdapterCrypto

Contract methods analysis:

`constructor(address,uint8) returns()`
Vulnerabilities not detected

`addLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`swap(address,uint256,address,address,uint256,uint8,uint8, address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`removeLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

8. adapters/crypto2/PoolAdapterCrypto

Contract methods analysis:

`constructor(address) returns()`
Vulnerabilities not detected

`addLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`swap(address,uint256,address,address,uint256,uint8,uint8, address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`removeLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

9. adapters/meta1/PoolAdapter.sol

Contract methods analysis:

`constructor(uint8) returns()`
Vulnerabilities not detected

`addLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`swap(address,uint256,address,address,uint256,uint8,uint8, address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`removeLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

10. adapters/stable1/PoolAdapter

Contract methods analysis:

constructor(address, uint8) returns()
Vulnerabilities not detected

addLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8, address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`removeLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

11. adapters/stable2/PoolAdapter

Contract methods analysis:

constructor(uint8) returns()
Vulnerabilities not detected

addLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8, address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`removeLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

12. adapters/stable3/PoolAdapterAave

Contract methods analysis:

`constructor(uint8) returns()`	
Vulnerabilities not detected	

`addLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`swap(address,uint256,address,address,uint256,uint8,uint8, address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

`removeLiquidity(address,uint256,address,address,uint256, uint8,address) returns(uint256)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

13. adapters/stable4/PoolAdapterStableNg

Contract methods analysis:

addLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

removeLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

14. VirtualPriceReceiver

Contract methods analysis:

`constructor(address,uint64[],address[]) returns()`
Vulnerabilities not detected

`receiveValidatedData(bytes4,address,uint64) returns(bool)`
Vulnerabilities not detected

`setAddressBook(address) returns()`
Vulnerabilities not detected

`setVirtualPriceSender(uint64,address) returns()`
Vulnerabilities not detected

`receiveVirtualPrice(uint256,uint256) returns()`
Vulnerabilities not detected

`getVirtualPriceEth() returns(uint256)`
Vulnerabilities not detected

`getVirtualPriceArb() returns(uint256)`
Vulnerabilities not detected

`getVirtualPriceBsc() returns(uint256)`
Vulnerabilities not detected

`getVirtualPricePol() returns(uint256)`
Vulnerabilities not detected

`getVirtualPriceAvax() returns(uint256)`
Vulnerabilities not detected

`getVirtualPriceOpt() returns(uint256)`
Vulnerabilities not detected

15. VirtualPriceSender

Contract methods analysis:

constructor(address) returns()
Vulnerabilities not detected

setAddressBook(address) returns()
Vulnerabilities not detected

setReceiver(address, uint64, address) returns()
Vulnerabilities not detected

sendVirtualPrice(address, uint64) returns()
Vulnerabilities not detected

`sendVirtualPrice(address[], uint64[]) returns()`
Vulnerabilities not detected

ACKNOWLEDGED	WARNING
`_sendVirtualPrice(address, uint64) returns()`	
Acknowledged: tx can be sandwiched, thus resulting in incorrect virtualPrice.	

Verification checksums

Contract name	Bytecode hash(SHA-256)
AddressBook	a955ee64cd37eae0d3c591f94295f6d7b4196a40c8146587be6f1bf7f12799c4
BaseRouter	664c4db353f84c9a90b542256a7c8db877bb3478cbc770e9873b71f2a6e8c06c
RouterV2	5fd8da0024c3aeddc1296fb874a841b14605ea53b83cd663a7a2c91d9a91c63f
SynthesisV2	6bc455b00f144c85f6a9df9e1f38f7c7649366b058695e7cf34104d797d9357a
ThirdPartySynthAdapter	dd77a214bea69f01b8e8b66ad2e870d0d5a01394cb16275c6ea65bef407192df
UnifiedRouterV2	eb3f55b3387ca443707921256b7df8b5cbfcc36bbb1c23255648d479c486e9d0
adapters/crypto1/PoolAdapterCrypto	df41ba0aabb26afbc69640f2408f56c826582f1035f046c1c4fc3adcbc41ccd1

Contract name	Bytecode hash(SHA-256)
adapters/crypto2/ PoolAdapterCrypto	336bca3de04f2e1ea6d98c9071ddfa9bb5b 0b8aedf8eefaeaf093241210f6417
adapters/meta1/ PoolAdapter.sol	fc6be076245427f968486e508453c20697f 568594d726e588fd2391d4fb7446d
adapters/stable1/ PoolAdapter	8403e0ce202bee95488ded4471e82d7125a 2209b12e7355b0db2372c108fccae
adapters/stable2/ PoolAdapter	71a17f1744c43501f859cc2747e41f98a8cd0d 9b4a2df27420eb2852a1f75bc7
adapters/stable3/ PoolAdapterAave	6708fe32370527b7d42c937950f8578eb4ff 9eca691cfe2dd8ccabe3a508c20e
adapters/stable4/ PoolAdapterStableNg	1901b527f0450a5f402d277b0c4e5a07e828 2641c644b3f9b16946e59cef902d
VirtualPriceReceiver	055d969dd65429262ab429a93b7bb0630d 117ba4fb87b71fb92e89e8b37e381a
VirtualPriceSender	d1ed799f2b46d486011d763aa83d558fd1d6 3afeeab9dd8b25e480f5f45b3935