Code4rena Review - Part 1

Concrete

HALBORN

Code4rena Review - Part 1 - Concrete

Prepared by: HALBORN

Last Updated 01/28/2025

Date of Engagement by: January 9th, 2025 - January 24th, 2025

Summary

98% ⓘ OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
46	0	13	27	6	0

TABLE OF CONTENTS

1. Introduction

Concrete engaged Halborn to conduct a review of the fixes applied as remediations for the Code4rena findings in the Blueprint project, beginning on **January 8th, 2025**, and ending on **January 24th, 2025**. The security assessment was scoped to the fixes implemented after the Code4rena contest (held from **November 15, 2024**, to **November 29, 2024**) for the sc_earn_v1 GitHub repository. The review focused on verifying the correctness of remediations for 46 prioritized findings out of 316 total submissions identified during the contest. Commit hashes and further details are outlined in the **Scope** section of this report.

2. Assessment Summary

Halborn was provided two weeks for the engagement and assigned one full-time security engineer to review the security of the smart contract in scope. The engineer is a blockchain and smart contract security expert with advanced penetration testing and smart contract hacking skills, and deep knowledge of multiple blockchain protocols.

The purpose of the assessment is to:

1. **Verify the remediations** for the 46 security findings marked for resolution.
2. **Ensure no new risks** were introduced by the applied fixes.

Halborn confirmed that **almost all security findings were properly addressed** by the Concrete team. The remediations adhered to best practices, and no critical regressions or unintended side effects were observed in the reviewed fixes.

3. SCOPE

FILES AND REPOSITORY

(a) Repository: 2024-11-concrete

(b) Assessed Commit ID: d2950ec

(c) Items in scope:

- src/claimRouter/ClaimRouter.sol
- src/factories/VaultFactory.sol
- src/interfaces/Constants.sol
- src/interfaces/DataTypes.sol
- src/interfaces/Errors.sol
- src/interfaces/IBeraOracle.sol
- src/interfaces/IClaimRouter.sol
- src/interfaces/IConcreteMultiStrategyVault.sol
- src/interfaces/IImplementationRegistry.sol
- src/interfaces/IMockProtectStrategy.sol
- src/interfaces/IMockStrategy.sol
- src/interfaces/IProtectStrategy.sol
- src/interfaces/IRewardManager.sol
- src/interfaces/IStrategy.sol
- src/interfaces/ISwapper.sol
- src/interfaces/ITokenRegistry.sol
- src/interfaces/IVaultDeploymentManager.sol
- src/interfaces/IVaultFactory.sol
- src/interfaces/IVaultRegistry.sol
- src/interfaces/IWithdrawalQueue.sol
- src/managers/DeploymentManager.sol
- src/managers/RewardManager.sol
- src/managers/VaultManager.sol
- src/queue/WithdrawalQueue.sol
- src/registries/ImplementationRegistry.sol
- src/registries/TokenRegistry.sol
- src/registries/VaultRegistry.sol
- src/strategies/Aave/AaveV3Strategy.sol
- src/strategies/Aave/DataTypes.sol
- src/strategies/Aave/IAaveV3.sol
- src/strategies/ProtectStrategy/ProtectStrategy.sol
- src/strategies/Radiant/DataTypes.sol
- src/strategies/Radiant/IRadiantV2.sol
- src/strategies/Radiant/RadiantV2Strategy.sol
- src/strategies/Silo/EasyMathV2.sol
- src/strategies/Silo/IBaseSiloV1.sol
- src/strategies/Silo/ISiloV1.sol

- src/strategies/Silo/SiloV1Strategy.sol
- src/strategies/StrategyBase.sol
- src/strategies/compoundV3/CompoundV3Strategy.sol
- src/strategies/compoundV3/ICompoundV3.sol
- src/swapper/OraclePlug.sol
- src/swapper/Swapper.sol
- src/vault/ConcreteMultiStrategyVault.sol
- src/strategies/Morpho/MorphoVaultStrategy.sol
- src/libraries/MultiStrategyVaultHelper.sol

Out-of-Scope: Security findings not reporting during the Code4rena contest.

REMEDIATION COMMIT ID:

- 1fb8be9
- 4b65e57
- 6ab7758
- 117c6a1
- ba85a57
- 7e7c6f0
- ed2b3e2
- ec89752
- 1ea392c
- 8b37dd8
- 3999efd
- fe9a822
- 8091626
- bd65fcd
- f437e01
- 1264593
- 2154622
- 8ea0b8c
- 67ad0e0
- a9c42a5
- 9cc780f
- a9f6857
- 2391dde
- 00c2c99
- 20f3ee5
- 4d8ac5c
- 1b76aff
- 2fbe22f
- 359bc35
- 6486ba4

- 0884170
- afdae9a
- 7b0fb13

Out-of-Scope: New features/implementations after the remediation commit IDs.

4. FINDINGS OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F36 - INCORRECT TOTAL ASSETS CALCULATION IN SILOV1STRATEGY	HIGH	SOLVED - 12/10/2024
C4-F38 - VAULTMANAGER DOESN'T IMPLEMENT FUNCTION TO CALL HARVESTREWARDS ON CONCRETEMULTISTRATEGYVAULT	HIGH	SOLVED - 12/09/2024
C4-F39 - MISSING VALIDATION FOR CTASSETTOKEN_ IN SWAPTOKENSFORREWARD ALLOWS ATTACKER TO DRAIN TREASURY ACCOUNT OF REWARD TOKENS	HIGH	SOLVED - 12/11/2024
C4-F6 - STRATEGIES INCLUDE HELD ASSETS AS PART OF THE TOTAL ASSETS, CAUSING LOSS OF FUNDS TO DEPOSITORS	HIGH	SOLVED - 12/09/2024
C4-F7 - RETIRING STRATS DOESN'T SEND FUNDS TO VAULT	HIGH	SOLVED - 12/10/2024
C4-F52 - DOS ATTACK ON WITHDRAW QUEUE	HIGH	SOLVED - 12/18/2024
C4-F28 - CLAIMROUTER ASSUMES EVERY CASCADE TOKEN HAS 6 DECIMALS	HIGH	SOLVED - 12/10/2024
C4-F25 - SWAPTOKENSFORREWARDS COULD QUOTE WRONG RATE	HIGH	SOLVED - 12/11/2024

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F48 - HARVESTREWARDS CAN'T HANDLE FEE-ON-TRANSFER TOKEN AS REWARD TOKEN	MEDIUM	SOLVED - 12/18/2024
C4-F60 - VALUE LEAK SENT TO USERS FROM PROTOCOL WHILE ROUNDING UP IN _WITHDRAWSTRATEGYFUNDS	MEDIUM	SOLVED - 12/12/2024
C4-F11 - PREVIEWMINT() RETURNS A WRONG VALUE	MEDIUM	SOLVED - 12/13/2024
C4-F30 - PAUSING AN EXTERNAL PROTOCOL THAT IS USED IN A STRATEGY DOSES THE WHOLE VAULT	MEDIUM	SOLVED - 12/13/2024
C4-F55 - PULLFUNDSFROMSINGLESTRATEGY DOESN'T CHECK FOR 0 STRATEGY BALANCE, FORCING CHANGEALLOCATIONS TO REVERT SOMETIMES	MEDIUM	SOLVED - 12/13/2024
C4-F62 - PROTECT STRATEGY DOESN'T ACCOUNT FOR ALLOCATIONS WHEN REQUESTING FUNDS AND REPAYING, LEADING TO UNEXPECTED REVERTS ON WITHDRAWAL	MEDIUM	SOLVED - 12/18/2024
C4-F22 - REMOVESTRATEGY() CAN BE DOSED BY SENDING 1 WEI TO THE TO-BE-DELETED STRATEGY	MEDIUM	SOLVED - 12/13/2024
C4-F51 - WITHDRAWAL QUEUE CAN BE SPAMMED, FORCING THE ADMIN TO HUGE GAS COSTS TO RESOLVE LEGIT WITHDRAW REQUESTS	LOW	SOLVED - 12/18/2024
C4-F21 - SHAREVALUE CAN BE INFLATED AND EARLY INVESTORS CAN BE CHARGED FOR PERFORMANCE THAT NEVER HAPPENED	MEDIUM	SOLVED - 12/11/2024
C4-F9 - SETVAULTBYTOKENLIMIT AND SETTOTALVAULTSALLOWED WILL NOT BE USABLE	MEDIUM	SOLVED - 12/12/2024

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F4 - VAULT USERS CAN CAUSE PERFORMANCE FEES TO ALWAYS BE CALCULATED BASED ON THE LOWEST TIER, REDUCING FEES FOR THE FEERECEIVER	MEDIUM	NOT SOLVED - 12/12/2024
C4-F14 - IF USER IS BLOCKLISTED FOR ANY OF THE REWARD TOKENS THEY WON'T BE ABLE TO WITHDRAW ASSETS FROM THE VAULT	MEDIUM	SOLVED - 01/19/2025
C4-F13 - WRONG ROUNDING DIRECTION WHEN APPLYING FEES	LOW	SOLVED - 12/13/2024
C4-F35 - USERS LOSES A PORTION OF THEIR DEPOSITS WHEN HARVESTING REWARDS FOR STRATEGIES WHERE THE REWARDTOKEN IS THE SAME AS THE ASSET MINTED BY THE PROTOCOL WHERE THE STRATEGY DEPOSITS FUNDS TO	HIGH	PARTIALLY SOLVED - 12/19/2024
C4-F47 - ATTACKERS CAN STEAL REWARDS BY FRONTRUNNING THE HARVESTING OF REWARDS AND MINTING HUGE AMOUNT OF VAULT'S SHARES TO REDUCE THE REWARDS PER SHARE	LOW	SOLVED - 12/19/2024
C4-F190 - PERFORMANCEFEE IS ACCIDENTALLY RETURNED IN SHARE UNITS INSTEAD OF ASSET UNITS	HIGH	SOLVED - 12/11/2024
C4-F173 - PROTOCOL ALWAYS ASSUMES 18 DECIMALS WHICH COMPROMISES THE CALCULATION OF THE PERFORMANCE FEE	HIGH	SOLVED - 12/12/2024
C4-F31 - A REPLACED PROTECT-STRATEGY CAN STEAL ALL THE FUNDS FROM THE VAULT	MEDIUM	SOLVED - 12/12/2024
C4-F40 - REWARD TOKEN SWAPPING ECONOMICS ARE FLAWED, ENABLING ATTACKS OR CAUSING LOSSES TO LPS DEPENDING ON MARKET CONDITIONS	HIGH	SOLVED - 12/11/2024
C4-F182 - TREASURY REWARD TOKENS DRAIN VIA REWARD RATE ARBITRAGE	HIGH	SOLVED - 12/11/2024

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F17 - INCORRECT COMPUTATION OF GETAVAILABLEASSETSFORWITHDRAWAL FROM STRATEGIES	MEDIUM	SOLVED - 12/16/2024
C4-F29 - AFTER A TOKEN IS UNREGISTERED ON THE TOKENREGISTRY, NO OTHER OPERATION CAN BE MADE FOR THAT TOKEN	MEDIUM	SOLVED - 12/11/2024
C4-F188 - USERS CAN AVOID PAYING WITHDRAWFEE BY USING THE SWAPPER	LOW	SOLVED - 12/11/2024
C4-F3 - TAKEFEES MODIFIER IS NOT USED ON ALL FUNCTIONS IT SHOULD BE, WHICH WILL LEAD TO LOSS OF FESS	MEDIUM	SOLVED - 12/13/2024
C4-F66 - BATCH WITHDRAWALS FROM WITHDRAWAL QUEUE CAN FAIL TO MARK THE LAST WITHDRAWAL REQUEST AS CLAIMED DUE TO OFF BY ONE ERROR	MEDIUM	SOLVED - 12/18/2024
C4-F42 - PREVIEWSWAPTOKENSFORREWARD DOES NOT CHECK TREASURY FOR ITS REWARD BALANCE	MEDIUM	SOLVED - 12/11/2024
C4-F259 - CALL TO WITHDRAW() REVERTS DUE TO ATTEMPT TO BURN MORE SHARES THAN ISSUED	LOW	SOLVED - 12/17/2024
C4-F288 - PROTOCOLFEE IS CHARGED EVEN FOR THE PAUSED DURATION	MEDIUM	SOLVED - 12/13/2024
C4-F18 - USE OF STRICT EQUALITY DISALLOWS ADDING NEW STRATEGY	MEDIUM	SOLVED - 12/13/2024
C4-F264 - CALL TO PAUSEALLVAULTS() FAILS IF ANY VAULT IS ALREADY IN PAUSED STATE	MEDIUM	SOLVED - 12/13/2024

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F23 - SWAPTOKENSFORREWARD IS LACK OF SLIPPAGE PROTECT	MEDIUM	SOLVED - 12/11/2024
C4-F50 - THE PROTOCOL CHARGES WITHDRAWFEE TO THE FEERECEIVER CAUSING FUNDS TO BECOME STUCK IN THE CONTRACT	MEDIUM	SOLVED - 12/13/2024
C4-F24 - MISSING ORACLE STALENESS CHECK ALLOWS PRICE MANIPULATION	MEDIUM	SOLVED - 12/11/2024
C4-F46 - UNREGISTERED REWARDTOKENS CAN STILL BE SWAPPED FOR REWARD	MEDIUM	SOLVED - 12/11/2024
C4-F192 - INCONSISTENT STATE MANAGEMENT ON REMOVETOKEN	MEDIUM	SOLVED - 12/11/2024
C4-F252 - LACK OF ALLOCATION VALIDATION DURING CONCRETEMULTISTRATEGYVAULT INITIALIZATION CAN RENDER VAULT NON-FUNCTIONAL	LOW	SOLVED - 12/14/2024
C4-F123 - DUST SHARES CHECK BYPASS THROUGH MINT FUNCTION	MEDIUM	SOLVED - 12/14/2024
C4-F58 - DEPOSIT LIMITS IN CONCRETEMULTISTRATEGYVAULT AND STRATEGYBASE ARE INEFFECTIVE	MEDIUM	SOLVED - 12/17/2024

Halborn strongly recommends conducting a follow-up assessment of the project either within six months or immediately following any material changes to the codebase, whichever comes first. This approach is crucial for maintaining the project's integrity and addressing potential vulnerabilities introduced by code modifications.