// Smart Contract Security Assessment 01.27.2025 - 02.10.2025

Code4rena Review - Part 2

Concrete

HALBORN

Code4rena Review - Part 2 - Concrete

Prepared by: HALBORN

Last Updated 02/12/2025

Date of Engagement by: January 27th, 2025 - February 10th, 2025

Summary

100% ⓘ OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
42	0	3	22	17	0

TABLE OF CONTENTS

1. Introduction

`Concrete` engaged Halborn to conduct a review of the disputed findings for the `Code4rena` contest in the Blueprint project, beginning on **January 27th, 2025**, and ending on **January 31st 2025**. The security assessment was scoped to the disputed findings after the Code4rena contest (held from **November 15, 2024**, to **November 29, 2024**) for the `sc_earn_v1` GitHub repository. The review focused on assessing the correctness of 42 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 **verify** the security findings marked as acknowledged, disputed or duplicated.

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:

- a9f6857
- 14c6707
- 8b37dd8

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

4. FINDINGS OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F8 - RADIANT STRATEGY'S REWARDS CAN NEVER BE CLAIMED	HIGH	RISK ACCEPTED - 01/29/2025
C4-59 - INSUFFICIENT WITHDRAWAL LIQUIDITY OF SOME STRATEGIES CAN BREAK USERS' LEGIT WITHDRAWALS	MEDIUM	RISK ACCEPTED - 01/29/2025
C4-F37 - _GETSTRATEGY DOES NOT ALWAYS SELECT THE CORRECT VAULT	MEDIUM	NOT APPLICABLE - 12/10/2024
C4-F45 - WITHDRAWALQUEUE BURNS USERS' SHARES WHILE STILL LENDING OUT THE USER'S ASSETS, CAUSING LOSS OF YIELD FOR USERS IN THE WITHDRAWAL QUEUE	LOW	RISK ACCEPTED - 01/24/2025

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F2 - _VALIDATEANDUPDATEDEPOSITTIMESTAMPS IS WRONGLY UPDATING FEESUPDATEDAT, RESETING THE ACCRUED PROTOCOL FEE	MEDIUM	NOT APPLICABLE
C4-F57 - WITHDRAWALQUEUE DOES NOT WORK WITH REBASING OR AIRDROP TOKENS	LOW	RISK ACCEPTED - 02/06/2025
C4-F16 - _ADDTOKENSTOSTRATEGY OF THE CLAIM ROUTER OPENS UP WAYS TO GAME PROTECT STRATEGIES	LOW	RISK ACCEPTED - 02/04/2025
C4-F61 - NEW WITHDRAWALS CAN BE EXECUTED BEFORE ANY OF THE ALREADY QUEUED WITHDRAWALS	MEDIUM	RISK ACCEPTED - 02/10/2025
C4-F32 - LACK OF SLIPPAGE PROTECTION	LOW	RISK ACCEPTED - 01/29/2025
C4-F65 - USER WITH BLUEPRINT CAN ADD REWARDS ON BEHALF OF A DIFFERENT BLUEPRINT	LOW	RISK ACCEPTED - 12/19/2024
C4-F19 - LOCKED USER FUNDS DUE TO INVALID LOGIC IN _WITHDRAWSTRATEGYFUNDS FUNCTIONS	MEDIUM	RISK ACCEPTED - 12/18/2024
C4-F295 - SHARE PRICE MANIPULATION THROUGH ASYNCHRONOUS DEBT RECORDING IN PROTECTSTRATEGY	HIGH	NOT APPLICABLE - 12/19/2024
C4-F237 - FLASH LOAN EXPLOIT ENABLES MANIPULATION OF REWARDS	HIGH	NOT APPLICABLE - 01/07/2025
C4-F306 - FORCED FREQUENT REWARD UPDATE MAY CAUSE LOSS OF ACCUMULATING REWARDS FOR SMALL-CAPITAL USERS	MEDIUM	NOT APPLICABLE - 12/13/2024

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F76 - FOR VAULTS WORKING WITH STRATEGIES THAT MINTS REBASING TOKENS FOR DEPOSITS, THE PERFORMANCE FEE WILL BE INCORRECTLY CHARGED TO ALL NEW DEPOSITS THAT ARE MADE IN BETWEEN TWO CALLS TO THE TAKEFEES() MODIFIER	LOW	NOT APPLICABLE - 02/01/2025
C4-F268 - STRATEGIES MIGHT HAVE UNINITIALIZED STATE	MEDIUM	FUTURE RELEASE - 01/30/2025
C4-F260 - NO WAY TO CREATE STRATEGIES FOR TOKENS WITH NON-STRING SYMBOL METHOD	MEDIUM	NOT APPLICABLE - 12/13/2024
C4-248 - WITHDRAWALS WILL BE TEMPORARILY DOSD IF A CERTAIN STRATEGY'S ALLOCATION IS SET TO 0	MEDIUM	NOT APPLICABLE - 01/03/2025
C4-F281 - NO MECHANISM IMPLEMENTED TO RETRIEVE REPAYED TOKENS FROM PROTECT STRATEGY TO CONCRETE VAULT	MEDIUM	NOT APPLICABLE
C4-F54 - CHANGING STRATEGIES ALLOCATIONS WITH LOCKED FUNDS IN STRATEGIES WILL BREAK ALLOCATION PERCENTAGES	LOW	RISK ACCEPTED - 01/28/2025
C4-F56 - EXECUTEBORROWCLAIM DOES NOT ACCOUNT FOR FEE ON TRANSFER TOKENS	LOW	RISK ACCEPTED - 02/06/2025
C4-F144 - ATTACKER CAN DOS ENTIRE VAULT, PREVENTING MAJORITY OF USERS FROM COMPLETING DEPOSITS	MEDIUM	RISK ACCEPTED - 02/10/2025
C4-F49 - INCORRECT REWARD ACCOUNTING INSIDE HARVESTREWARDS() IF TOKENHELPER.ATTEMPTSAFETRANSFER() FAILS	MEDIUM	SOLVED - 12/19/2024
C4-F20 - TIERED FEE NOT CHARGED FOR UPPER BOUNDARY VALUES	MEDIUM	SOLVED - 12/19/2024

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F266 - REMOVESTRATEGY NEED TO CLAIM REWARDS BEFORE REMOVAL	LOW	RISK ACCEPTED - 12/27/2024
C4-F191 - ACCRUEDPERFORMANCEFEE USE A OUT-OF-DATE HIGHWATERMARK	MEDIUM	NOT APPLICABLE - 12/14/2024
C4-F113 - RADIANT STRATEGY'S LACK OF FALLBACK MECHANISMS CREATES SINGLE POINT OF FAILURE RISK	LOW	RISK ACCEPTED - 12/14/2024
C4-F99 - EXPLOITATION OF MINIMAL DEBT IN PROTECTION STRATEGIES LEADING TO UNFAIR REWARD DISTRIBUTION	LOW	RISK ACCEPTED - 12/14/2024
C4-F15 - LOSS OF REWARD WHEN EVER A USER WITHDRAWS FROM THE STRATEGIES AS FUNDS ARE REMOVED BEFORE THE REWARD IS CLAIMED/UPDATED LEADING TO A LOSS OF REWARD FOR THE AMOUNT WITHDRAWN	MEDIUM	NOT APPLICABLE - 12/14/2024
C4-F10 - THE PROTOCOL CHARGES WITHDRAWFEE TO THE FEERECEIVER, CAUSING FUNDS TO BECOME STUCK IN THE CONTRACT	MEDIUM	SOLVED - 12/13/2024
C4-F172 - BORROW FLOW CLAIM FEES NOT IMPLEMENTED	MEDIUM	NOT APPLICABLE - 12/14/2024
C4-F122 - WHALES CAN PREVENT USERS WITHDRAWING ASSETS AND REDEEMING SHARES	MEDIUM	RISK ACCEPTED - 02/10/2025
C4-F64 - CONCRETEMULTISTRATEGYVAULT.MINT() CAN FAIL DUE TO ROUNDING UP THE STRATEGY DEPOSIT AMOUNT	MEDIUM	SOLVED - 12/19/2024
C4-F223 - IMMUTABLE PROXY WITH UPGRADEABLE CONTRACT	MEDIUM	FUTURE RELEASE - 01/30/2025

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
C4-F90 - BORROW FLOW VAULT SELECTION ALGORITHM LEADS TO INEFFICENT USE OF LIQUIDITY AND UNFAIR DISTRIBUTION OF RISK BETWEEN LPS	LOW	RISK ACCEPTED - 01/01/2025
C4-F63 - BROKEN FUNCTIONALITY IN CONCRETEMULTISTRATEGY VAULT ON ZERO ALLOCATION STRATEGY	LOW	NOT APPLICABLE - 12/23/2024
C4-F247 - HUGE PRECISION LOSS IN PROTECTSTRATEGY'S HIGHWATERMARK CALCULATION BREAKS STRATEGY SELECTION LOGIC	MEDIUM	NOT APPLICABLE
C4-F53 - STRATEGIES WITH CERTAIN TOKENS CANNOT BE REMOVED	LOW	RISK ACCEPTED - 01/20/2025
C4-256 - NO ZERO CHECK ON PRICES FROM THE BERACHAIN ORACLE	LOW	RISK ACCEPTED - 12/20/2024
C4-F265 - REMOVEREWARDTOKEN() FAILS TO CLAIM THE PENDING REWARDS TOKENS BEFORE REMOVING THEM FROM THE VAULT	LOW	RISK ACCEPTED - 12/21/2024
C4-F5 - PREVIEWREDEEM AND PREVIEWDEPOSIT DON'T MATCH REDEEM AND DEPOSIT RESPECTIVELY	LOW	RISK ACCEPTED - 01/17/2025
C4-F1 - RECEIVER_ OF CONCRETEMULTISTRATEGYVAULT.DEPOSIT FUNCTION CALL CAN UNFAIRLY GAIN MORE SHARES THAN RECEIVER_ OF CONCRETEMULTISTRATEGYVAULT.MINT FUNCTION CALL WHEN DEPOSITING SAME AMOUNT OF ASSETS	MEDIUM	NOT APPLICABLE - 01/17/2025

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.