yAudit Euler Combined Cantina Audit Fixes Review

Auditors:

- adriro
- Invader-tak

Table of Contents

m 448. A call with empty calldata may have unexpected behavior

n 490. `BalanceUtils.transferBalance` may give the wrong info to the hook

o 477. PegStabilityModule fees and rounding

p 368. An attacker can plummet a share price when there are little funds in the vault

q 75. Dust clean in `transferBorrow()` could lead to accounting errors

r 68. Consider adding `address(this)` balance to ignored supply in ESynth

s 254. `indexed` Keyword in Events Causes Data Loss for String Variables

t 207. `protocolFeeShare()` might return a value different than the actual used value

u 43. Panic when liquidating worthless liability

v 508. Panic when liquidating worthless liability

w 331. EulerSavingsRate: Lack of early interest accruals due to precision loss

x 67. EVault introduces strange checks, which makes it a weird token

y 320. `setImplementation` is not checking if the `newImplementation` is contract

z 520. Governor may accidentially break the liquidation logic

aa 443. New EVault deployment and configuration mechanism can be tricked to gain advantages

ab 141. In `setLTV()`, attempt to price the collateral in order to detect self-collateral config mistake

ac 196. Malicious controllers make EVC compatible tokens intrinsically susceptible to reentrancy

Review Summary

Euler v2 Cantina audit competition fixes review

Two yAudit security engineers were contracted to review fixes to audit findings from the Euler v2 Cantina audit competition. Their task was to meticulously examine the implemented changes and ensure that all identified issues were properly addressed. In addition to reviewing the fixes, the auditors also assessed various enhancements and other miscellaneous updates and fixes that were included. This comprehensive review, conducted over the month of July, aimed to enhance the security and reliability of the Euler v2 platform by leveraging independent auditors' expertise to validate the improvements' effectiveness.

Scope

The Cantina contest covered issues related to several projects, ensuring a thorough examination and resolution of vulnerabilities. The fixes were implemented and can be found in the following repositories:

- evc-cantina-fixes
- reward-streams-cantina-fixes
- epo-cantina-fixes
- evk-cantina-fixes

These repositories contain the detailed changes and enhancements made to address the issues identified during the audit competition.

yAudit and the auditors, committed to transparency, make no warranties regarding the security of the code and do not warrant that the code is free from defects. yAudit and the auditors do not represent nor imply to third parties that the code has been audited nor that the code is free from defects. By deploying or using the code, Euler and users of the contracts agree to use the code at their own risk.

EVC issues

41. Contracts cannot be upgraded

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The issue's relevance is unclear, but the "fix" is acceptable since the members in the domain structure are optional.

Additional Fixes

N/A

102. metadata is not reset to original value when execution context is restored

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The updated description is clear, and Kasper correctly notes that metadata fields aren't used in TransientStorage.

Additional Fixes

N/A

103. specs and implementation of call & batch function is not matching

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The updated description is clear; it's just a spec update.

Additional Fixes

N/A

173. Mismatch between whitepaper and code

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The updated description is clear; it's just an update to the whitepaper.

Additional Fixes

N/A

196. Malicious controllers make EVC compatible tokens intrinsically susceptible to reentrancy

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. EVC-compliant tokens are susceptible to reentrancy attacks. The issue is out of scope, but the proposal has been implemented.

Additional Fixes

N/A

213. Update comments to accurately reflect the whitepaper and the code

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The docs update is clear.

Additional Fixes

N/A

483. Redundant calls to `getAddressPrefixInternal()`

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Gas optimization change.

Additional Fixes

N/A

516. An attacker can exploit the EVC account system to steal Euler vault tokens from users

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. We agree with devs that the attack has a very low probability.

Additional Fixes

Highlighted an issue in which the operator could still bypass the patch, which is now fixed in a4dcf9e.

Enhancement. Add `onlyEVCAccountOwner` modifier

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

No issues were spotted in the enhancement.

Additional Fixes

N/A

Reward Streams issues

31. Neither `MAX_EPOCHS_AHEAD` and `MAX_DISTRIBUTION_LENGTH` enforces the restrictions by themselves

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The issue is about a weak validation, but it seems to have no major impact. The team has acknowledged that these are soft checks intended to prevent mistakes.

Additional Fixes

N/A

154. Users can not use their non-owner sub-account as the recipient in `unstake()`

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Transfers were initially only allowed to the EVC owner of an account to prevent the loss of funds. Now, they have relaxed this condition and allow transfers if the token is EVC-compatible.

Additional Fixes

N/A

167. Potential Permanent Loss of Rewards when there's no staker

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The updated documents are clear and detail the impact on rewards with no other significant effects. There is a rounding issue in the division between rewards and epoch duration when there are no stakers, but its impact appears to be minimal.

Additional Fixes

N/A

231. Setting `forfeitRecentReward` during balance increase would actually grant the user more rewards

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Calls to the hook that should set forfeit rewards to true (when `isControlCollateralInProgress()` is true) always decrease the balance, so the new change shouldn't override them.

Additional Fixes

N/A

233. Setting `forfeitRecentReward` to true during `claimReward()` doesn't actually forfeit anything

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Changes to documentation are clear.

Additional Fixes

N/A

240. Inconsistent Duration Validation

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Changes to documentation are clear.

Additional Fixes

N/A

273. `registerReward()` can be DOS-ed after a very long time due to block gas limit

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Changes to documentation are clear.

Additional Fixes

N/A

313. There are some typos in reward readme docs

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Typos fixed.

Additional Fixes

N/A

339. The comment contains an incorrect variable and is misleading

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Typos fixed.

Additional Fixes

N/A

Enhancement. DistributionStorage refactor

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

The refactoring looks okay. It seems better now since the global accumulator type is aligned with the account's accumulator type.

Additional Fixes

N/A

EPO issues

118. Certain addresses are not compatible with `_getDecimals`

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Setting a reserved range should fix the issue, no edge cases found in the range.

Additional Fixes

N/A

205. Uniswap oracle are very easy to manipulate on L2

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Changes to documentation are clear.

Additional Fixes

N/A

443. New EVault deployment and configuration mechanism can be tricked to gain advantages

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Additional safeguards have been added to prevent interaction on a new vault before it is fully configured.

Additional Fixes

N/A

EVK issues

OZ. OpenZeppelin synth fixes

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

The order of storage updates during withdrawals of the ESR is incorrect. It should update the `totalAssets` variable before the transfer (i.e., before the internal call to `_withdraw()`). The issue has been fixed in PR#19.

Additional Fixes

N/A

Enhancement. Remove ERC20Collateral, add ERC20EVCCompatible

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK. Remove the need to enforce checks at the ESynth level as the wrapping vault will enforce the checks and be used as collateral. This also removes the need for reentrancy checks in the ESynth contract since there are no callbacks now.

Additional Fixes

N/A

Enhancement. Change `transferFrom` method order

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK. Possibly increased gas usage.

Additional Fixes

N/A

Enhancement. Remove unnecessary check for 0 length symbol/names

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK.

Additional Fixes

N/A

Enhancement. Remove ESR collateral feature

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK. Fixes the state order update in PR#1.

Additional Fixes

The non-reentrant modifier can be removed as well.

Enhancement. Remove `clearLTV` function

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK.

Additional Fixes

There is still a section in the whitepaper that refers to this feature.

Enhancement. Prevent a potential IRM underflow

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK.

Additional Fixes

N/A

Enhancement. Move deposit call to module for contract size

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK.

Additional Fixes

N/A

Enhancement. Use gov modifier from EVC in EVK (based on PR#19)

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK. Added the modifier to the ownable accessible functions in the ESynth contract.

Additional Fixes

N/A

Documentation. Specs update

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK. Documentation update.

Additional Fixes

N/A

Documentation. Whitepaper update

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK. Documentation update.

Additional Fixes

N/A

Documentation. Cantina docs fixes

Cantina Report (N/A) Euler team fix

Severity

N/A

Auditors Notes

Fix OK. Documentation update.

Additional Fixes

N/A

448. A call with empty calldata may have unexpected behavior

Cantina Report Euler team fix

Severity

N/A

Auditors Notes

Fix OK.

Additional Fixes

N/A

490. `BalanceUtils.transferBalance` may give the wrong info to the hook

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK.

Additional Fixes

N/A

477. PegStabilityModule fees and rounding

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Adjusted rounding based on direction.

Additional Fixes

N/A

368. An attacker can plummet a share price when there are little funds in the vault

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Manipulation is mitigated by adding a minimum liability to allow for debt socialisation. There could be additional side effects from this, but none were found.

Additional Fixes

N/A

75. Dust clean in `transferBorrow()` could lead to accounting errors

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Fixed unchecked overlow while logging the debt.

Additional Fixes

N/A

68. Consider adding `address(this)` balance to ignored supply in ESynth

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK.

Additional Fixes

N/A

254. `indexed` Keyword in Events Causes Data Loss for String Variables

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK.

Additional Fixes

N/A

207. `protocolFeeShare()` might return a value different than the actual used value

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Replicate fee logic used in `convertFees()`.

Additional Fixes

N/A

43. Panic when liquidating worthless liability

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Check when liability is 0 to prevent reverts due to division by 0. Other divisions also look okay, considering PR#24.

Additional Fixes

N/A

508. Panic when liquidating worthless liability

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Same as issue #43.

Additional Fixes

N/A

331. EulerSavingsRate: Lack of early interest accruals due to precision loss

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The change skips the last time update when accrued is zero, but it stills considers the update in `gulp()` if `updateInterestAndReturnESRSlotCache()` didn't. This is a good approach.

Additional Fixes

N/A

67. EVault introduces strange checks, which makes it a weird token

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Self-approval is allowed, but this doesn't update the state, so `allowance[x][x]` would still return 0.

Additional Fixes

N/A

320. `setImplementation` is not checking if the `newImplementation` is contract

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK.

Additional Fixes

N/A

520. Governor may accidentially break the liquidation logic

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Prevents a division by zero.

Additional Fixes

N/A

443. New EVault deployment and configuration mechanism can be tricked to gain advantages

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. Hook target is `address(0)` at initialization so all operations will revert.

Additional Fixes

N/A

141. In `setLTV()`, attempt to price the collateral in order to detect self-collateral config mistake

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The bug is interesting but looks like an impossible setup.

Additional Fixes

N/A

196. Malicious controllers make EVC compatible tokens intrinsically susceptible to reentrancy

Cantina Report Euler team fix

Severity

Low.

Auditors Notes

Fix OK. The EVK `checkAccountStatus()` has been updated to be a view function, following the change in the EVC.

Additional Fixes

N/A
