CHAINSECURITY

A brand of Decentralized Security AG

contact@chainsecurity.com,
@chain_security,
https://chainsecurity.com/

18 June 2021

Smart Contract Bug Report

Status: The bug has not been exploited

Dear Enzyme Council,

With the following letter we would like to give an overview about a bug detected by the Avantgarde Finance team, the impacts thereof and the steps performed to mitigate the identified risk.

A bug in the *PerformanceFee* Smart Contract has been detected. To fix this bug, it was necessary to redeploy a fixed version of this contract. To allow existing vaults to switch to this updated version, an upgrade to a new release of Enzyme is necessary too. Any upgrade of the Enzyme Protocol requires vaults to actively upgrade in order to switch to the new version.

Issue:

Vaults affected by the issue are vaults featuring a denomination asset with decimals other than 18 (which is non-standard) and the Performance Fee active. This is a minority of all vaults.

The bug, due to a unit mismatch, if exploited using carefully crafted parameters would have allowed to mint shares outstanding for the vault manager as the performance of the vaults is incorrectly assessed. However, note that the vault manager is a trusted role.

The main concern was that the bug could have been triggered by any external party. While this actor wouldn't benefit financially it could have been used to harm the system. Excess shares minted would lower the value of the current shares of the vault.

Actions performed:

In order to mitigate the issue all four affected primitive assets have been temporarily removed from the asset universe on May 6th. Since this action in the afternoon of May 6th the bug cannot be triggered anymore. However, due to this the operation of affected vaults and for all vaults trades involving these assets became limited. Another temporary hotfix allows continuation of trading of these assets for otherwise unaffected vaults.

The following steps were taken to mitigate the implications of the issue:

1) The primitive assets not having 18 decimals were removed for the time being from the asset universe of the current Enzyme release on May 6th at 14:37 UTC. This removed the possibility of the bug being exploited to harm the system

2) The implementation of the performance fee was fixed

3) Both Performance and Management fees were settled actively by the Enzyme operators for all the affected vaults before the assets were removed. Due to the removed assets, this would not be possible during migration. For these vaults, migration must be initiated with the bypass failure flag enabled. This ensures that these fees have been settled correctly recently

4) A new release of the affected Smart Contract for Enzyme was deployed in the late afternoon of May 7th.

5) The new release is now ready to go-live which requires the approval of the Enzyme Council. After the new release is live, vaults can migrate to the new release and continue normally

During the transition phase we have performed the following additional procedures:

1) We checked the whole code for similar issues and could not identify any similar circumstances

2) We assessed the proposed fixes as well as the migration process for any possible side effects and intended functionality and could not identify any (major) findings

3) We analysed for possible issues due to the inconsistent state of the Enzyme system upon failure of fee settlement during migration and could not identify such issues

4) We verified that the deployed contracts match the verified commit and are configured correctly. Please note that the configuration check is restricted to making sure the different contracts are correctly linked together and that basic constructor parameters are correct. We couldn't verify more advanced state changes for which we didn't have a full specification. Upon request we are happy to provide the full details of the deployment check

The verified code commit is: ce0fd40ae5edfdd1c28bcf41a79f9682ef290e0e

New releases are a rare event and allow major code changes in the smart contracts of Enzyme. The need to update to a new release in order to fix the bug has been used by the developers to introduce some other small outstanding changes, namely:

- Using *SafeApprove* in the VaultLib
- Removal of the forced settlement of Synthetix in the Integration Manager – this significantly reduces the gas usage for all calls on adapters
- Removal of the enforcement that spent assets are either tracked or a supported asset of the system. This now allows the fully trusted vault managers to trade away unsupported reward or airdrop token
- An enhanced check that only supported asset can be added manually by the fully trusted vault manager

We'd like to note that after all affected vaults have upgraded to the new release, the affected assets could be readded to the current release which would allow all other vaults to restart to operate normally without the need to update to the new release.

We like to express our gratitude to you for your trust in us and are available should have any further questions.

Sincerely yours,

The ChainSecurity Team