On Jan 26th, Anchor bETH integration had been migrated from using the Shuttle bridge to the Wormhole bridge. The upgrade lacked smart contract API versioning, allowing two users to send the total of 443.56111857 webETH (Terra-side Wormhole bETH) to inaccessible Terra addresses. The corresponding stETH tokens are currently locked in the AnchorVault Ethereum contract. The recap of the incident is included at the end of the post.

The affected users have been refunded from the dev team's funds. Refunding the dev team by unlocking stETH from the AnchorVault contract requires changes to the AnchorVault smart contract. Those are already implemented and the migration is scheduled for 12PM UTC — 2PM UTC, Feb 10th, 2022. During that time, both AnchorVault smart contract and anchor.lido.fi UI would be disabled.

The cleanest possible course of actions includes burning tokens on inaccessible Terra addresses. Terra-side token contract (webETH) is managed by the Wormhole Protocol, so any actions on this side require the governance proposal. We're exploring the possible course of actions, but there's no defined & clear ETAs now. We're proposing to go ahead on Ethereum side first. Note that if the governance proposal for burning webETHs has passed, the changes made to AnchorVault internal calculations have to be rolled back.

Migration implements the following AnchorVault changes:

1. Adding the method to refund dev team finance multisig wallet 0x48F300bD3C52c7dA6aAbDE4B683dEB27d38B9ABb

by releasing stETH corresponding to the webETH locked on Terra and adding internal calculation tweaks to account for the operation.

1. Adding versioning for user-facing methods, allowing to break backwards compatibility on upgrades & preventing the core cause of the incident from resurfacing again. The rationale and mechanics are described in LIP-10 with tweaks allowing to bump version upon delegate changes.

2. Adding emergency stop method accessible from the dev team's multisig. Resuming the integration would require the DAO vote.

3. The method to roll back calculation tweaks after the burning of the Terra-side webETH tokens on inaccessible addresses (requires favourable Wormhole governance decision).

The PR with code changes can be checked out here:https://github.com/lidofinance/anchor-collateral-steth/pull/21

Note that the pull request lists InsuranceConnector changes according toLIP-6 along the things included to V3. They don't require AnchorVault tweaks, but depend on the Lido protocol upgrade, so won't be included on Feb 10th migration.

While the full postmortem is to be prepared & posted in the nearest time, a short incident recap is:

- The UI for converting from stETH/ETH to bETH that interacts with the AnchorVault contract was disabled.
- The AnchorVault contract was upgraded to use the new bridge. The upgrade changed the semantics of the AnchorVault.submit method used for conversion: the _terra_address: bytes32 argument started requiring left zero padding of the 20-byte address instead of right padding.
- The new UI implementing left zero padding of Terra addresses was deployed and enabled.
- Two users were able to send AnchorVault.submit transactions using the outdated UI, either because they had a browser tab with the old UI open or due to the browser caching issues. These transactions (0xc875f85f525d9bc47314eeb8dc13c288f0814cf06865fc70531241e21f5da09d, 0x7abe086dd5619a577f50f87660a03ea0a1934c4022cd432ddf00734771019951) contained Terra addresses encoded using right zero padding.
- The Wormhole bridge decoded the right-padded Terra addresses incorrectly (since it expects left padding), minting the wrapper webETH tokens to unreachable addresses, effectively burning the tokens.