Zellic

Smart Contract Update Review

December 14, 2022

Prepared for:

Stargate

Prepared by:

Jasraj Bedi and Kate Belotskaia

Zellic Inc.

About Zellic

Zellic was founded in 2020 by a team of blockchain specialists with more than a decade of combined industry experience. We are leading experts in smart contracts and Web3 development, cryptography, web security, and reverse engineering. Before Zellic, we founded perfect blue, the top competitive hacking team in the world. Since then, our team has won countless cybersecurity contests and blockchain security events.

Zellic aims to treat clients on a case-by-case basis and to consider their individual, unique concerns and business needs. Our goal is to see the long-term success of our partners rather than to simply provide a list of present security issues. Similarly, we strive to adapt to our partners' timelines and to be as available as possible. To keep up with our latest endeavors and research, check out our website zellic.io or follow @zellic_io on Twitter. If you are interested in partnering with Zellic, please email us at hello@zellic.io or contact us on Telegram at https://t.me/zellic_io.

1 Introduction

We were asked to review an update to Stargate FeeLibrary and a minor patch to the router. The FeeLibrary update added custom handling for depegged stablecoin states. The router patch fixed a lingering issue in stargate that would cause a revert when performing a callback to a non-existent address.

1.1 Scope

The engagement involved a review of the following targets:

proof-lib

Repository	https://github.com/ryanzarick/stargate/
Versions	Router.sol (`3e69c2754dca70c0032d1468c3da105b8b885584`) StargateFeeLibraryV05.sol (`ad9e4f0799d2a71b31ed2cac8560e312dcbc52a6`)
Type	Solidity
Platform	Ethereum (and other compatible chains)

Contact Information

The following consultants were engaged to conduct the assessment:

Jasraj Bedi, Co-founder
jazzy@zellic.io

Kate Belotskaia, Senior Security Engineer
kate@zellic.io

1.2 Disclaimer

This assessment does not provide any warranties on finding all possible issues within its scope; i.e., the evaluation results do not guarantee the absence of any subsequent issues. Zellic, of course, also cannot make guarantees on any additional code added to the assessed project after our assessment has concluded. Furthermore, because a single assessment can never be considered comprehensive, we always recommend multiple independent assessments paired with a bug bounty program. Finally, this assessment report should not be considered as financial or investment advice.

2 Fee Library Update (v05.1)

The Stargate Fee Library was updated to version 5 to account for depegged stable coins causing imbalanced pools. The driving force behind the update is prevent toxic cross-chain swaps during depegging of stablecoins that leave Stargate in an imbalanced state. This imbalanced state requires the intervention of the foundation reset by injecting liquidity to rebalance pools.

2.1 Price states

For every stable pair pool, there are now three price-deviation states (normal, drift, depeg):

```
Normal State: ≥ $0.999 (10bps away from 1:1)
Drift State: $0.999 > p > $0.985: drift fee applicable.
Depeg State: ≤ $0.985: stop all cross-asset transactions from with the
    depegged token.
```

Price is set permissionlessly and is retrieved from a Chainlink oracle (10bps or 900s heartbeat sensitivity). The price drift (PD) is calculated upon price reaching or being lower than 0.999 (entering Drift state), and upon any change greater than 1bps when in Drift state. This is propagated to all associated fee libraries on other chains.

The oracle price updates happen on the BSC network and are propagated over to the other chains leveraging the LayerZero network. Thus, the Chainlink oracle on BSC is the ground truth source of price feeds.

A few minor concerns are listed as follows:

Stale Price Updates: The price updates could be mis-ordered by a relayer. By a crafting a message that fails in LzReceive, it could be later retry-ed causing the library to use stale prices. It was possible as the application was a `nonBlockingLzApp`, allowing out-of-order execution of packets. This was fixed in commit bc84e482 by using blocking `lzApp` instead.

PoolIDs collision on multiple chains: The current architecture assumes `poolId` on distinct chains signify the same asset type. This is not implemented as a protocol level invariant, but a deployment decision. As new pools are added, it is essential to make sure that this invariant holds to prevent poolId collisions when updating prices.

Code Complexity: The v5 library supports all types of pools but the depegging pro-

tection only applies to stable pools. This has caused the code to be unnecessarily complicated. It could be simplified by breaking the library into separate components. As Stargate supports per pool libraries, it would reduce the attack surface by having finer grained control and lower impact radius in case of a compromise. Simplifying the code also makes it less prone to bugs and/or missed edge cases.

3 Stargate Router

The Stargate router was updated to handle callbacks to non existent contract addresses. This patch prevents the whole transaction from reverting when the destination address is not a contract. This was thoroughly reviewed by the Zellic team and no issues were found.