Zellic

Highlight

Smart Contract Feature Review

July 4, 2022

Prepared for:

Kevin Matthews

Highlight, Inc.

Prepared by:

Ayaz Mammadov and Vlad Toie

Zellic Inc.

Contents

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 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 additional feature to the Highlight protocol, namely, the addition of supporting crypto payments. We reviewed 1 commit in the 'hl-contracts' repository. We did not find any issues in the introduced code.

1.1 Scope

The engagement involved a review of the following targets:

Crypto Payments

Repository https://github.com/highlightxyz/hl-contracts/

Versions `4727b738a6356ab0654b3edae7c2652e1a54d9e4`

Files

CentralPaymentsManager.sol

3b9b365aa6cfd57765e7b3caceb3a69ea669e1b5087150bd893290b7446df847

MaticWETH.sol

0bf5d58c2881a28c0d7ad51c883f82ef4696af26fcf53999cf0a9583a20e9450

IMinimalForwarder.sol

cf6f89938689a4e92dfa77e05f9ad545d1b06e121b3c62304bece42fc5be7239

INativeMetaTransaction.sol

0d8d4d3d4a9798c93692d5b9c404111179e6a3ccbac1913b7ad9a2f6933c6d25

IPermissionsRegistry.sol

8e40d508b1f93b276342b89c8242fc3b7477ddf6d1f2946272292b60e05c83d5

PermissionsRegistry.sol

cfe03b05fa32cf85795ebe004a41ca2a9d0ca9c9fc5d2ba3919799eb2d177f42

Type Solidity

Platform Polygon

Contact Information

The following consultants were engaged to conduct the assessment:

Ayaz Mammadov, Engineer
ayaz@zellic.io

Vlad Toie, Engineer
vlad@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 financial or investment advice.

2 Crypto Payments review

The crypto payments addition to the Highlight ecosystem was added to facilitate the purchase of community tokens/NFTs using crypto-currencies, this was done by using tokens that supported the ERC-2771 Meta Transaction system (meta txs), doing so, given the correct data a token would execute an action on the behalf of a user granted the signatures provided were correct. We did not find any issues in the introduced code.

A Central Payment Manager was added The `CentralPaymentsManager.sol` is the gateway to the crypto payments system, restricted to `onlyPlatformExecutor`, the quantaties of the transfers are calculated off-chain, and then are used along side with the user signatures to execute meta txs, and then a Highlight approved signature transfers the appropriate amount of community tokens to the recipient.