Zellic

LayerZero

Smart Contract Patch Review

November 22, 2022

Prepared for:

Ryan Zarick

LayerZero

Prepared by:

Katerina 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 a minor patch to the LayerZero ULNv2. The patch fixed a minor issue with dappRadar's usage of ULN. We did not find any issues with the patch.

1.1   Scope

The engagement involved a review of the following targets:

ULNv2 dappRadar

Repository	https://github.com/LayerZero-Labs/LayerZero-internal
Versions	d9a93e853e20d5f9da74e0fc85b818b1279a8b05
Files	/radar/contracts/UltraLightNodeV2Radar.sol
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

Katerina Belotskaia, Co-founder
stephen@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 Patch Review

The patch itself is an update to the ULNv2 contract specifically to accomodate the legacy design of dappRadar. The changes are summarized below:

Nonce upgrade dappRadar enforced LayerZero's nonce on their own contract. With the ULNv2 upgrade, the nonce at ULN would reset to 0, breaking dappRadar's logic. This patch reads the legacy nonce value and force increments new nonce to the legancy value