SHERLOCK

Security Review For LayerZero

Collaborative Audit Prepared For:	LayerZero
Lead Security Expert(s):	0x52 sammy
Date Audited:	April 7 - April 9, 2025
Final Commit:	80867a4

Introduction

OneSig is a smart contract solution designed to streamline the signing and execution of arbitrary 'calldata' on any EVM compatible blockchains.

Scope

Repository: sherlock-scoping/LayerZero-Labs__OneSig

Audited Commit: 80867a4e58ee6fcec4bb9e548eb5d37742bfb3f1

Final Commit: 80867a4e58ee6fcec4bb9e548eb5d37742bfb3f1

Files:

- packages/onesig-evm/contracts/MultiSig.sol
- packages/onesig-evm/contracts/OneSig.sol

Final Commit Hash

80867a4e58ee6fcec4bb9e548eb5d37742bfb3f1

Findings

Each issue has an assigned severity:

- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.
- High issues are directly exploitable security vulnerabilities that need to be fixed.
- Low/Info issues are non-exploitable, informational findings that do not pose a security risk or impact the system's integrity. These issues are typically cosmetic or related to compliance requirements, and are not considered a priority for remediation.

Issues Found

High	Medium	Low/Info
0	0	0

Issues Not Fixed and Not Acknowledged

High	Medium	Low/Info
0	0	0

Disclaimers

Sherlock does not provide guarantees nor warranties relating to the security of the project.

Usage of all smart contract software is at the respective users' sole risk and is the users' responsibility.