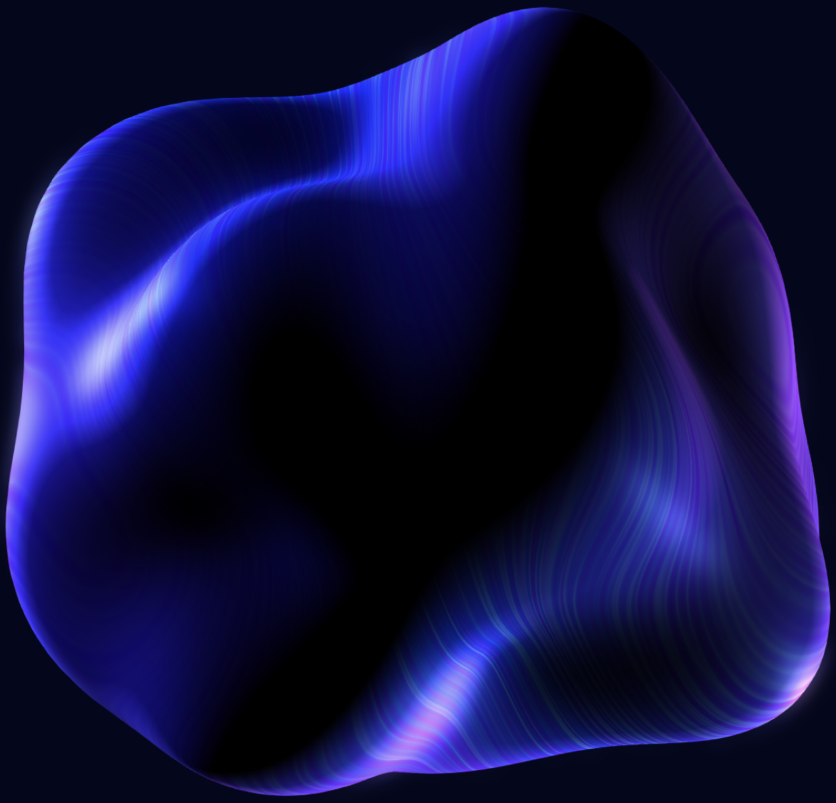
MUNDUS SECURITY

# Zerolend Deployment Check on zkSync Era



ZeroLend

# ZeroLend deployment check

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.
The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

## Project overview

ZeroLend is a lending protocol operating on zkSync Era chain. ZeroLend integrates lending logic by Aave with price oracles by Pyth Network.

## Reference information

| | |
|---|---|
| Name | ZeroLend |
| Language | Solidity |
| Chain | zkSync Era |
| Website | https://zerolend.xyz/ |
| Documentation | https://docs.zerolend.xyz/ |

# Scope of work

| # | contract | address |
|---|---|---|
| 1 | AaveOracle | 0x785765De3E9ac3D8eEb42B4724A7FEA8990142B8 |
| 2 | ACLManager | 0x9A60cce3da06d246b492931d2943A8F574e67389 |
| 3 | AToken | 0xe8178fF950Ea1B69a51cE961C542a4CC6Cb6e38E |
| 4 | DelegationAwareAToken | 0x102699803F4A2b02046C38C672401759af633510 |
| 5 | EmissionManager | 0x72D2aB433526d32e6Ee52c03d1562A9E79bf0F19 |
| 6 | IncentivesV2-Implementation | 0x86bd524C09508df7B4B9027464975351B1BC2c92 |
| 7 | IncentivesProxy | 0x54AB34aB3C723bD2674c7082aA6fFcdfd3A5BEdc |
| 8 | Pool-Implementation | 0x54d6F91bE4509826559ad12E1Ca6CA3A6C3811e0 |
| 9 | Pool-Proxy | 0x4d9429246EA989C9CeE203B43F6d1C7D83e3B8F8 |
| 10 | PoolConfigurator-Implementation | 0x8FBC873afD2a23D0bDd79d8a8756a38adda40810 |
| 11 | PoolConfigurator-Proxy | 0x9C3058F7bfCA6139ac3013999F57D7aa6a3AB1Ed |
| 12 | PoolDataProvider | 0xB73550bC1393207960A385fC8b34790e5133175E |
| 13 | ReservesSetupHelper | 0xe00d794744e763BeC67BdEdF6e852D4e0d958DFb |
| 14 | ReserveStrategy-rateStrategy StableOne | 0x70cA80C5dE9fC8f080a494453dF1aA9180073031 |
| 15 | ReserveStrategy-rateStrategy StableTwo | 0xcaA502e289bFb924732f44f5E70bd08fc052aab8 |
| 16 | ReserveStrategy-rateStrategy VolatileOne | 0xEdAc06D73DbdD3460B5728E4bBE9862b04Ac198a |
| 17 | StableDebtToken | 0x3A8ea541597D74ACB33F94533D731940AF516031 |
| 18 | UiIncentive DataProviderV3 | 0x91ccF57c1E9A7F5A9537eE59306faF8dA3b7e960 |
| 19 | UiPoolDataProviderV3 | 0x8FE0ac76b634B7D343Bd32282B98E9f271B43367 |

| # | contract | address |
|---|---|---|
| 20 | VariableDebtToken | 0xA48aCc9847Cc1dD2caDA05151C9A78Ba47a305Cb |
| 21 | WalletBalanceProvider | 0xdeEa10da04D867e3303AB6E50FA26C2d8a5e9f70 |
| 22 | WrappedTokenGatewayV3 | 0x767b4A087c11d7581Ac95eaFfc1FeBFA26bad3d2 |
| 23 | PoolAddressesProvider | 0x4f285Ea117eF0067B59853D6d16a5dE8088bA259 |
| 24 | USDC-USD | 0x75D018f04f9cb37936530F7e3A909474565A2467 |
| 25 | WETH-USD | 0x517F9cd13fE63e698d0466ad854cDba5592eeA73 |
| 26 | USDT-USD | 0xCf58E8e67F2BcDd977e61bB6FDC1B0EEd6E1939d |
| 27 | BorrowLogic | 0x81D6b98Beb0A4288dCFab724FDeaE52E5Aa2F7b1 |
| 28 | BridgeLogic | 0x6CDe8a8cEE9771A30dE4fEAB8eaccb58cb0d30aF |
| 29 | ConfiguratorLogic | 0x8731d4E5b990025143609F4A40eC80Fb482E46A0 |
| 30 | EModeLogic | 0xD84E953a621bb9D81Dc998E0b1482D2916153c23 |
| 31 | FlashLoanLogic | 0x424C0995114a614c12506D9A994d3eE140742f12 |
| 32 | LiquidationLogic | 0x8855Fd7d577A05d04Cea2E026c5BAa4Bb47feAf9 |
| 33 | PoolAddresses<br>ProviderRegistry | 0x78B93fBb35C97b32C7381C81Fa3A620b3fB7787B |
| 34 | PoolLogic | 0xA8D16FB0620E3376093cb89e2cD9dEF9fE47Daaa |
| 35 | SupplyLogic | 0x9223dC9205Cf8336CA59bA0bD390647E62D487E5 |
| 36 | Treasury-Controller | 0x677C3Cae4F23142c6A8480694554751B462d7326 |
| 37 | Treasury-Implementation | 0xC59971Ff27806629D9935fbFBBFC2236961f82C8 |
| 38 | TreasuryProxy | 0xE52540DBD350c611A1B9c51E97e2A6bc16c09133 |
| 39 | WETH-AToken | 0x9002ecb8a06060e3b56669c6B8F18E1c3b119914 |
| 40 | WETH-StableDebtToken | 0x9c9158BFF47342A20b7D2Ac09F89e96F3A209b9B |
| 41 | WETH-VariableDebtToken | 0x56f58d9BE10929CdA709c4134eF7343D73B080Cf |
| 42 | USDC-AToken | 0x016341e6Da8da66b33Fd32189328c102f32Da7CC |
| 43 | USDC-StableDebtToken | 0x5faC4FD2e4bCE392d34600d94Aa1114274e54Dff |

| # | contract | address |
|---|---|---|
| 44 | USDC-VariableDebtToken | 0xE60E1953aF56Db378184997cab20731d17c65004 |
| 45 | USDT-AToken | 0x9ca4806fa54984Bf5dA4E280b7AA8bB821D21505 |
| 46 | USDT-StableDebtToken | 0x6F977fD05962d67Eb7B16b15684fbEa0462F442d |
| 47 | USDT-VariableDebtToken | 0xa333c6FF89525939271E796FbDe2a2D9A970F831 |
| 48 | Timelock | 0x861cC6724D0aA7Ec7a868887643e682b1c16aeeC |
| 49 | Multisig ⚠ (see id-69) | 0x7b08d0d9D6f450243500338C39B1c9F01a30d801 |
| 50 | GhoToken | 0x90059C32Eeeb1A2aa1351a58860d98855f3655aD |
| 51 | GhoOracle | 0x1E3720185512d22C7352759e79dC3515d752AA50 |
| 52 | cbETH-USD | 0x3D5BcB12800A092FC85Ca00837594146F274C273 |
| 53 | BUSD-USD | 0x1a963D0C6bF364C1C8AE4F17b6aB773c627cEFB7 |
| 54 | PEPE-USD | 0xCd16A63d1960Afe718c4FE62D0b8D8f19Fc29618 |
| 55 | WBTC-USD | 0xe99FFA17f20F3f8022862d1BD13519D305eF1377 |
| 56 | uniV2LP-USD | 0x071Bf614bc2c50140c1f094346774e529571A9Fb |
| 57 | TransferStrategy | 0xc0fcea0b31c79f70b5453a9c70e361fcaccb43a2 |
| 58 | PEPE-AToken | 0x54330D2333AdBF715eB449AAd38153378601cf67 |
| 59 | LUSD-AToken | 0xd97Ac0ce99329EE19b97d03E099eB42D7Aa19ddB |
| 60 | WBTC-AToken | 0x7c65E6eC6fECeb333092e6FE69672a3475C591fB |
| 61 | BUSD-AToken | 0xb727F8e11bc417c90D4DcaF82EdA06cf590533B5 |
| 62 | GhoAToken Implementation | 0x0e1d2c6284144d60dda047c982d5389c5db052c5 |
| 63 | ONEZ-AToken | 0x52846A8D972ABbF49F67d83d5509aa4129257F46 |
| 64 | GhoVariableDebtToken Implementation | 0x6e8667e11bfefe57560f4b29f4d32440d856612b |
| 65 | ONEZ-VariableDebtToken | 0x77dcEd4833E3a91437Ed9891117BD5a61C2AD520 |
| 66 | BUSD-VariableDebtToken | 0x3E1F1812c2a4f356d1b4FB5Ff7cca5B2ac653b94 |
| 67 | GhoDiscountRateStrategy | 0x8c58628c4a67906cc09d33f65d34775c1ad9d19a |
| 68 | MultisigNew-Implementation | 0x1727c2c531cf966f902E5927b98490fDFb3b2b70 |
| 69 | MultisigNew-Proxy ⚠ (see id-49) | 0x1890f9204882dfa1b8f0aeaf56ae9b2ed149d18d |

| # | contract | address |
|---|---|---|
| 70 | z0KNC-USDC-USDT-AToken-zkSync | 0xed9fDA0a27088aec9C925d99D64ec168960ebF52 |
| 71 | z0KNC-eUSDC-USDT-AToken-zkSync-1 ⚠ (see id-72) | 0x2A039bBA9C29AA71Ba4DafB8b1EBc2D8C7A06df8 |
| 72 | z0KNC-eUSDC-USDT-AToken-zkSync-2 ⚠ (see id-71) | 0x2B1BBe3ba39B943eEEf675d6d42607c958F8d20f |
| 73 | z0SWORD-AToken-zkSync-1 ⚠ (see id-74) | 0xD9032b559595c81bfEceb4d2073D1ab248506749 |
| 74 | z0SWORD-AToken-zkSync-2 ⚠ (see id-73) | 0xDB87A5493e308Ee0DEb24C822a559bee52460AFC |
| 75 | z0VC-AToken-zkSync | 0x1f2dA4FF84d46B12f8931766D6D728a806B410d6 |
| 76 | z0MUTE-AToken-zkSync | 0xc3b6D357e0BeADb18A23a53E1dc4839C2D15bdC2 |
| 77 | z0DAI-AToken-zkSync | 0x15b362768465F966F1E5983b7AE87f4C5Bf75C55 |
| 78 | EarlyZerolend | 0x9793eac2fECef55248efA039BEC78e82aC01CB2f |
| 79 | MUTE-USD | 0x1dff8c0886ec6eb2fe6cbe060bf84e402516101f |
| 80 | SWORD-USD | 0x65b28bafdb15dd3cb47a568fba27fabb5b7d99d4 |
| 81 | DAI-USD | 0xf531672c92ad4658c54b4fbe855029df43c57390 |
| 82 | uniV2LP-USD-2 | 0x68b5d2d4037a78d676dd204cf45912003b3288ac |
| 83 | EarlyZero-USD ⚠ (see id-90) | 0x89b89884f4f8f6bfaf245c9bbec6ecbba3bcd969 |
| 84 | VC-USD | 0x29b08a8a8324884ee5eeb6e28e7274ee0e17980e |
| 85 | WBTC-VariableDebtToken-zkSync | 0xabd3c4e4ac6e0d81fcfa5c41a76e9583a8f81909 |
| 86 | DAI-VariableDebtToken-zkSync | 0x0325f21eb0a16802e2bacd931964434929985548 |
| 87 | LUSD-VariableDebtToken-zkSync | 0x41c618cce58fb27caf4eeb1dd25de1d03a0daac6 |
| 88 | StableDebtToken-zkSync-2 | 0xa04222ccb20e8b6cc2a45856e7f6ef14995bbdb9 |
| 89 | GhoVariableDebtToken-Implementation-2 | 0xd4ed3f810b4d28daf85bd1a0a52e09a7c05ff915 |
| 90 | EarlyZero-Oracle-2 ⚠ (see id-83) | 0x1bB24651CF854D44bA33A32dE09D595Da4faa8D1 |

# Table of contents

# Findings summary

## Storage findings - 1

| # | contract | storage issues<br>initial check |
|---|---|---|
| 2 | ACLManager-zkSync | found |
| 5 | EmissionManager | found |
| 13 | ReservesSetupHelper | found |
| 22 | WrappedTokenGatewayV3 | found |
| 33 | PoolAddressesProviderRegistry | found |
| 57 | TransferStrategy | found |
| 65 | ONEZ-VariableDebtToken-zkSync | found |
| 78 | EarlyZerolend | found |
| 83 | EarlyZero-USD | found |
| 90 | EarlyZero-Oracle-2 | found |

# Deployment check: storage

We thoroughly examine both public and private storage, as well as immutable and constant variables, to ensure that there are no misconfigurations, especially:

1. Incorrect or outdated addresses to other smart contracts referenced in the scope of work (SoW) - this includes addresses stored in variables, mappings, and other data structures.
2. Any references to other smart contracts or externally owned accounts (EOAs) that may be incorrect or outdated.
3. Any incorrect protocol settings stored in variables or other data structures.
4. Misconfigurations related to the roles and permissions of the contract.
5. Governance issues that may impact the operation and business logic of the smart contract.

## Statistics by issue type

| **type** | **comment** | **# found** |
|---|---|---|
| EOA | Externally-owned account possesses some kind of privileged access to a contract imposing centralization risks on the protocol. | 7 |
| incorrect value | Any kind of incorrect or unassigned values of contract's storage. | 4 |
| **total** | | 11 |

# ID-2. ACLManager-zkSync

| issue # | issue type |
|---|---|
| 1 | EOA |

1. EOA https://explorer.zksync.io/address/0x0f6e98a756a40dd050dc78959f45559f98d3289d possesses EMERGENCY_ADMIN role.

# ID-5. EmissionManager

| issue # | issue type |
|---|---|
| 1 | incorrect value |
| 2 | EOA |

1. _owner = 0x7b08d0d9d6f450243500338c39b1c9f01a30d801 -- old Multisig
2. _emissionAdmins, mapping(address => address) - EOAs

**NOTE:** EOAs are marked with ⚠.

| reward | admin |
|---|---|
| 0x5AEa5775959fBC2557Cc... | 0xb76F765A785eCa438e1d... ⚠ |
| 0x9793eac2fECef55248ef... | 0xb76F765A785eCa438e1d... ⚠ |

# ID-13. ReservesSetupHelper

| issue # | issue type |
|---|---|
| 1 | incorrect value |

1. _owner = 0x7b08d0d9d6f450243500338c39b1c9f01a30d801 -- old Multisig

# ID-22. WrappedTokenGatewayV3

| issue # | issue type |
|---|---|
| 1 | incorrect value |

1. _owner = 0x7b08d0d9d6f450243500338c39b1c9f01a30d801 -- old Multisig

# ID-33. PoolAddressesProviderRegistry

| issue # | issue type |
|---|---|
| 1 | incorrect value |

1. _owner = 0x7b08d0d9d6f450243500338c39b1c9f01a30d801 -- old Multisig

# ID-57. TransferStrategy

| issue # | issue type |
|---|---|
| 1 | EOA |
| 2 | EOA |

1. rewardsAdmin = b76f765a785eca438e1d95f594490088afaf9acc -- EOA
2. rewardsVault = b76f765a785eca438e1d95f594490088afaf9acc -- EOA

# ID-65. ONEZ-VariableDebtToken-zkSync

| issue # | issue type |
|---|---|
| 1 | incorrect value |

1. _incentivesController = 0x86bd524c09508df7b4b9027464975351b1bc2c92 -- logic address
    - MUST BE 0x54ab34ab3c723bd2674c7082aa6ffcdfd3a5bedc -- storage address

# ID-78. EarlyZerolend

| issue # | issue type |
|---|---|
| 1 | EOA |

1. _owner = 0xb76f765a785eca438e1d95f594490088afaf9acc -- EOA

# ID-83. EarlyZero-USD

| issue # | issue type |
|---|---|
| 1 | EOA |

1. _owner = 0xb76f765a785eca438e1d95f594490088afaf9acc -- EOA

# ID-90. EarlyZero-Oracle-2

| issue # | issue type |
|---|---|
| 1 | EOA |

1. _owner = 0xb76f765a785eca438e1d95f594490088afaf9acc -- EOA

# Disclaimers

## Mundus disclaimer

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

## Technical disclaimers

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.