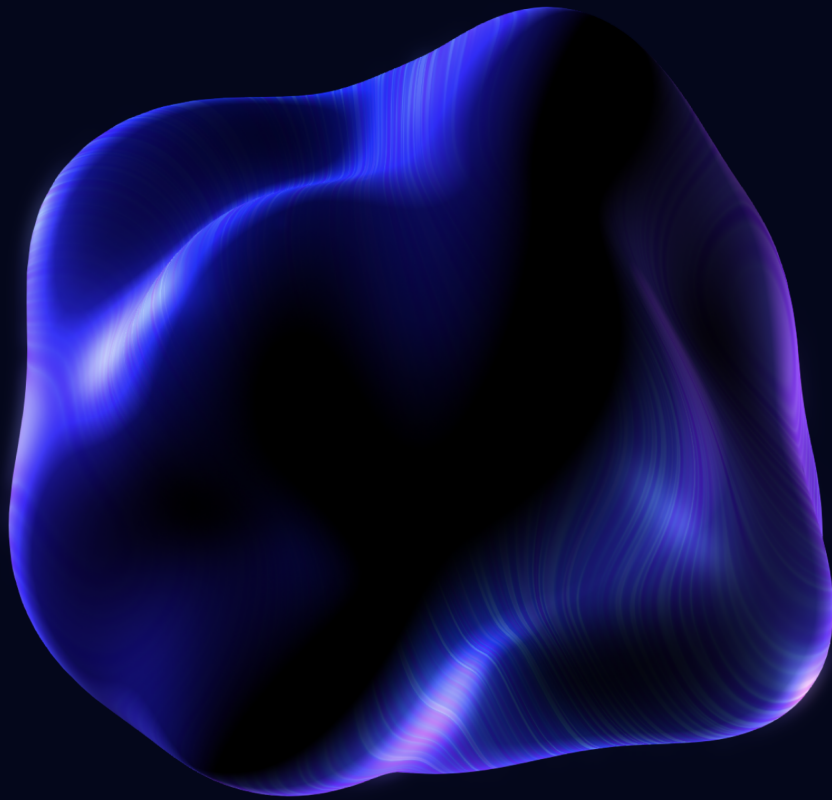




MUNDUS  
SECURITY

# Zerolend Deployment Check on Linea Network



 **ZeroLend**



[mundus.dev](https://mundus.dev)



[@mundus\\_security](https://twitter.com/mundus_security)



[Mundus.dev](https://Mundus.dev)



# 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	Linea
Website	<a href="https://zerolend.xyz/">https://zerolend.xyz/</a>
Documentation	<a href="https://docs.zerolend.xyz/">https://docs.zerolend.xyz/</a>



# Scope of work

#	contract	address
1	AaveOracle-linea	0xff679e5b4178a2f74a56f0e2c0e1fa1c80579385
2	ACLManager-linea	0xb2178109a414c3a869e5104283fcf1a18923d0b8
3	AToken-linea	0xd2a2a567674e85bedab9dcc402bcae6c4e0aabb8
4	DelegationAwareAToken-linea	0xf49ee3ea9c56d90627881d88004aabdfc44fd82c
5	EmissionManager	0x749df84fd6de7c0a67db3827e5118259ed3abba5
6	IncentivesProxy	0x28f6899ff643261ca9766ddc251b359a2d00b945
7	IncentivesV2-Implementation	0x6e9d0ce24d14fb1750ba0369e300413b230ca947
8	Pool-Implementation	0x8676e39b5d2f0d6e0d78a4208a0ccbc50504972e
9	Pool-Proxy-linea	0x2f9bb73a8e98793e26cb2f6c4ad037bdf1c6b269
10	PoolAddressesProvider-linea	0xc44827c51d00381ed4c52646aeadb45b455d200eb
11	PoolAddressesProviderRegistry	0x5046c3c0d7a362709df433d5431d64973c7f08cb
12	PoolConfigurator- Implementation	0x78ad3d53045b6582841e2a1a688c52be2ca2a7a7
13	PoolConfigurator-Proxy-linea	0xf17218b09699d0f7145e40e771e72130ff616498
14	PoolDataProvider-linea	0x67f93d36792c49a4493652b91ad4bd59f428ad15
15	ReservesSetupHelper	0xb8634e0a320d0f4861062514a63b659e52a87e21
16	ReserveStrategy- rateStrategyStableOne	0xaa999ea356f925bf1e856038c5d182ae5e8a4973
17	ReserveStrategy- rateStrategyStableTwo	0xb7ed499e7570ee7691eef4df9d708d258de2b512
18	ReserveStrategy- rateStrategyVolatileOne	0x0f9bfa294be6e3ca8c39221bb5dfb88032c8936e
19	StableDebtToken-linea	0x859c2ca97ead2742a0758bc9dd889e9d0e7e84e8
20	Treasury-Controller	0x59423cceb710266520db98034ff62dd1e2090e10
21	Treasury-Implementation	0xcccf56e2b6ad4c06af8214781b77cd98446377bf
22	TreasuryProxy	0x89fec31dad373922879bd6279ccdc3666c5d1b7a



#	contract	address
23	UiIncentiveDataProviderV3	0xcbbdc0aed7cdf2472784068abef23a902cafabbb98
24	UiPoolDataProviderV3	0x81b3184a3b5d4612f2c26a53da8d99474b91b2d2
25	VariableDebtToken-linea	0x0a8058203387c15a711204908ed9efed9f76e6a8
26	WalletBalanceProvider	0xe05361ea51e20118072aec0fb0fd178e8b09d69e
27	WrappedTokenGatewayV3	0x5d50be703836c330fc2d147a631cdd7bb8d7171c
28	BorrowLogic	0xd85bbd487b957857d10d7d96f3a08f6bab55f7e3
29	BridgeLogic	0xc3b6ddc1c9876a922754f1d01d18893c7956a74d
30	ConfiguratorLogic	0x9660b39d0e38be0f7e09cc6c516bd335746262ee
31	EModeLogic	0xb0b0b1d3c0f9823c13d4e0481e86387baff452a2
32	FlashLoanLogic	0x15785c5d383fa33339cf5d5720546c24313bc66d
33	LiquidationLogic	0x7fab93af49ce663dbc2f94bc4def5c84d6605663
34	PoolLogic	0x9698fdf843cbe4531610ac231b0047d9ffc13bc6
35	SupplyLogic	0x5e35d90db7118c2ae96a8de458401986879bb0ef
36	GRAI-AToken-linea	0xe7e54ca3d6f8a5561f8cee361260e537bdc5be48
37	GRAI-StableDebtToken-linea	0x7c2e57764ec33292fe098636aaa5d0357d814d16
38	GRAI-VariableDebtToken-linea	0xe6b9b00d42fa5831cce4e44d9d6d8c51ba17cd1e
39	MAI-AToken-linea	0x759cb97fbc452bafd49992ba88d3c5da4dd9b0e7
40	MAI-StableDebtToken-linea	0xb8e26f3c4afb4f56f430a390dc3f3b12f8a50b26
41	MAI-VariableDebtToken-linea	0xc1d9ca73f57930d4303d380c5dc668c40b38598b
42	USDC-AToken-linea	0x2e207eca8b6bf77a6ac82763eed2a94de4f081d
43	USDC-StableDebtToken-linea	0xd07e6a4da4e360ba6edde42ce7867051ea4be024
44	USDC-VariableDebtToken-linea	0xa2703dc9fbaccd6ec2e4cbfa700989d0238133f6
45	USDT-AToken-linea	0x508c39cd02736535d5cb85f3925218e5e0e8f07a
46	USDT-StableDebtToken-linea	0x607f422f2e2de0fd1b084223ed16ae51c2453b06
47	USDT-VariableDebtToken-linea	0x476f206511a18c9956fc79726108a03e647a1817



#	contract	address
48	WETH-AToken-linea	0xb4ffef15daf4c02787bc5332580b838ce39805f5
49	WETH-StableDebtToken-linea	0x27c7733d7a0f142720af777e70ebc33ca485d014
50	WETH-VariableDebtToken-linea	0xcb2da0f5aece616e2cbf29576cfc795fb15c6133
51	AToken-linea-2	0xb83e5027829fe9691ca0688012bcf1189176e1b5
52	HypernativeTrigger	0x608382bb732156fe2324817b3f45c92325a30e41
53	ListingContract-1	0x4c076e26b86b819b214b54ab8f26188bdf3df531
54	ListingContract-2	0xf0180aff10456beb855eab7d62ce8c00ebe7dfae
55	GnosisSafeProxy	0x14aAD4668de2115e30A5FeeE42CFa436899CCD8A
56	GnosisImplementation	0x3e5c63644e683549055b9be8653de26e0b4cd36e

# Table of contents

1. Findings summary
2. Deployment check: storage
3. Disclaimers

## Findings summary

### Storage findings

#	contract	storage issues initial check
2	ACLManager-linea	found
5	EmissionManager	found
15	ReservesSetupHelper	found
20	Treasury-Controller	found
52	HypernativeTrigger	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.	5
Incorrect values	Incorrectly set parameters of the protocol introducing potential flaws in execution logic	1
total		6



## ID-2. ACLManager

issue #	issue type
1	Incorrect values

- Two listing contracts possess `ASSET_LISTING_ADMIN`, one of them may be superfluous
  - `0x4c076e26b86b819b214b54ab8f26188bdf3df531`
  - `0xf0180aff10456beb855eab7d62ce8c00ebe7dfae`

## ID-5. EmissionManager

issue #	issue type
1	EOA

- `_emissionAdmins, mapping(address => address)` - EOAs

**NOTE:** EOAs are marked with ⚠.

reward	admin
<code>0x40a59a3f3b16d9e74c81...</code>	<code>0xf6e98a756a40dd050dc...</code> ⚠
<code>0x78354f8dcc269a615a7...</code>	<code>0xf6e98a756a40dd050dc...</code> ⚠

## ID-15. ReservesSetupHelper

issue #	issue type
1	EOA

- `_owner = 0xf6e98a756a40dd050dc78959f45559f98d3289d` -- EOA



## ID-20. Treasury-Controller

issue #	issue type
1	EOA

```
1. _owner = 0xf6e98a756a40dd050dc78959f45559f98d3289d -- EOA
```

## ID-52. HypernativeTrigger

issue #	issue type
1	EOA
2	EOA

```
1. EOA 0x9ad0395264c7c45b0486e5890cf794c2774c1540 possesses RISK_MANAGER role
2. EOA 0x0323acd6062b463c205fb2e76ca020ddae0d8e98 possesses RISK_MANAGER role
```

# 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.