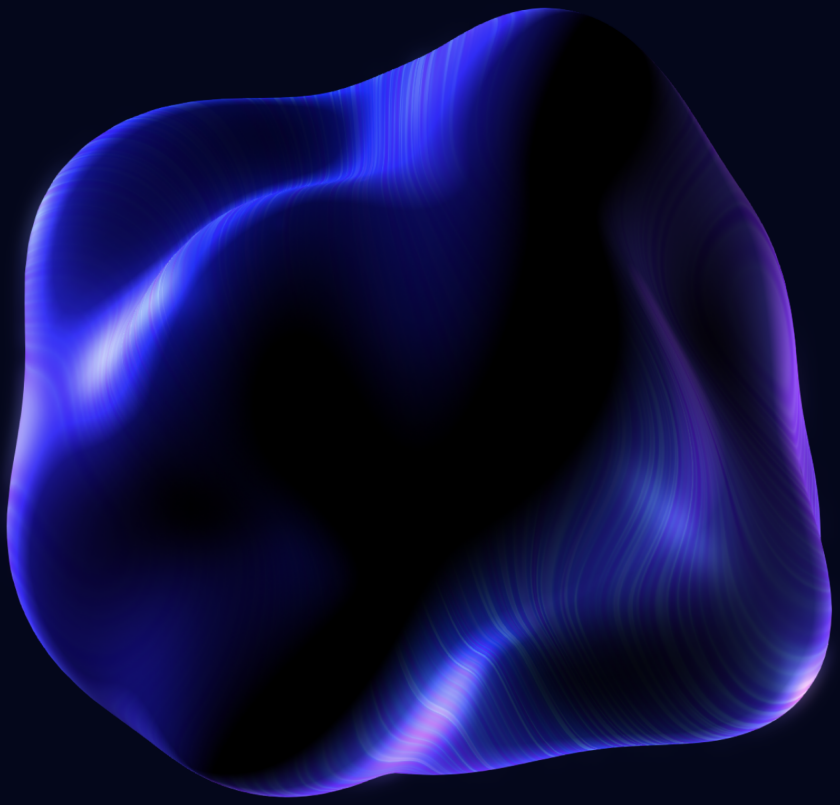
MUNDUS
SECURITY

Zerolend Deployment Check on Manta Network



ZeroLend

MUNDUS
SECURITY

ZeroLend deployment check

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	Manta
Website	https://zerolend.xyz/
Documentation	https://docs.zerolend.xyz/

MUNDUS
SECURITY

Scope of work

#	contract	address
1	AaveOracle	0xff679e5b4178a2f74a56f0e2c0e1fa1c80579385
2	ACLManager	0xb2178109a414c3a869e5104283fcf1a18923d0b8
3	AToken	0xd2a2a567674e85bedab9dcc402bcae6c4e0aabb8
4	DelegationAwareAToken	0xf49ee3ea9c56d90627881d88004aabdfc44fd82c
5	EmissionManager	0x749df84fd6de7c0a67db3827e5118259ed3abba5
6	IncentivesProxy	0x28f6899ff643261ca9766ddc251b359a2d00b945
7	IncentivesV2-Implementation	0x6e9d0ce24d14fb1750ba0369e300413b230ca947
8	Pool-Implementation	0x8676e39b5d2f0d6e0d78a4208a0ccbc50504972e
9	Pool-Proxy	0x2f9bb73a8e98793e26cb2f6c4ad037bdf1c6b269
10	PoolAddressesProvider	0xc44827c51d00381ed4c52646aeab45b455d200eb
11	PoolAddressesProviderRegistry	0xc3b6ddc1c9876a922754f1d01d18893c7956a74d
12	PoolConfigurator-Implementation	0x78ad3d53045b6582841e2a1a688c52be2ca2a7a7
13	PoolConfigurator-Proxy	0xf17218b09699d0f7145e40e771e72130ff616498
14	PoolDataProvider	0x67f93d36792c49a4493652b91ad4bd59f428ad15
15	PullRewardsTransferStrategy	0x2acc2b9fc1123ab649895c9e825260f31348732b
16	ReservesSetupHelper	0xb8634e0a320d0f4861062514a63b659e52a87e21
17	ReserveStrategy-rateStrategyStableOne	0xaa999ea356f925bf1e856038c5d182ae5e8a4973
18	ReserveStrategy-rateStrategyStableTwo	0xb7ed499e7570ee7691eef4df9d708d258de2b512
19	ReserveStrategy-rateStrategyVolatileOne	0x0f9bfa294be6e3ca8c39221bb5dfb88032c8936e
20	StableDebtToken	0x859c2ca97ead2742a0758bc9dd889e9d0e7e84e8
21	Treasury-Controller	0x3fc90e521397b251d4aaa1fbeac7cc32f25e78fa

#	contract	address
22	Treasury-Implementation	0xadc1eb4e8c72f03339638a7b43b2097fc1afb6c8
23	TreasuryProxy	0x97e59722318f1324008484aca9c343863792cbf6
24	UiIncentiveDataProviderV3	0x81b3184a3b5d4612f2c26a53da8d99474b91b2d2
25	UiPoolDataProviderV3	0xa32eb787f2a3dc1f2c2da0e5d8cae7ff74e6fd32
26	VariableDebtToken	0x0a8058203387c15a711204908ed9efed9f76e6a8
27	WalletBalanceProvider	0xcbdc0aed7cdf2472784068abef23a902cafabb98
28	WrappedTokenGatewayV3	0xe05361ea51e20118072aec0fb0fd178e8b09d69e
29	BorrowLogic	0x9698fdf843cbe4531610ac231b0047d9ffc13bc6
30	BridgeLogic	0xcccf56e2b6ad4c06af8214781b77cd98446377bf
31	ConfiguratorLogic	0x2f7e54ff5d45f77bffa11f2aee67bd7621eb8a93
32	EModeLogic	0x59423cceb710266520db98034ff62dd1e2090e10
33	FlashLoanLogic	0xb0811a1fc9fb9972ee683ba04c32cb828bcf587b
34	LiquidationLogic	0x89fec31dad373922879bd6279ccdc3666c5d1b7a
35	PoolLogic	0xc6df4dddbfacb866e78dcc01b813a41c15a08c10
36	SupplyLogic	0x15785c5d383fa33339cf5d5720546c24313bc66d
37	MATIC-AToken	0x2e207eca8b6bf77a6ac82763eeed2a94de4f081d
38	MATIC-StableDebtToken	0xd07e6a4da4e360ba6edde42ce7867051ea4be024
39	MATIC-VariableDebtToken	0xa2703dc9fbaccd6ec2e4cbfa700989d0238133f6
40	TIA-AToken	0x508c39cd02736535d5cb85f3925218e5e0e8f07a
41	TIA-StableDebtToken	0x607f422f2e2de0fd1b084223ed16ae51c2453b06
42	TIA-VariableDebtToken	0x476f206511a18c9956fc79726108a03e647a1817
43	USDC-AToken	0xb4ffef15daf4c02787bc5332580b838ce39805f5
44	USDC-StableDebtToken	0x27c7733d7a0f142720af777e70ebc33ca485d014
45	USDC-VariableDebtToken	0xcb2da0f5aece616e2cbf29576cfc795fb15c6133
46	USDT-AToken	0x759cb97fbc452bafd49992ba88d3c5da4dd9b0e7
47	USDT-StableDebtToken	0xb8e26f3c4afb4f56f430a390dc3f3b12f8a50b26
48	USDT-VariableDebtToken	0xc1d9ca73f57930d4303d380c5dc668c40b38598b

#	contract	address
49	WBTC-AToken	0xe7e54ca3d6f8a5561f8cee361260e537bdc5be48
50	WBTC-StableDebtToken	0x7c2e57764ec33292fe098636aaa5d0357d814d16
51	WBTC-VariableDebtToken	0xe6b9b00d42fa5831cce4e44d9d6d8c51ba17cd1e
52	WETH-AToken	0x0684fc172a0b8e6a65cf4684edb2082272fe9050
53	WETH-StableDebtToken	0xffa256ad2487c4d989c3dfa6a6e9c13fe33beba4
54	WETH-VariableDebtToken	0xcc7b5fd2f290a61587352343b7cf77bb35cb6f00
55	wstETH-AToken	0x0ab214f127998a36ce7ab0087a9b0d20adc2d5ad
56	wstETH-StableDebtToken	0x28d7246cd9da102c75faa7d4cf1c5399b323f084
57	wstETH-VariableDebtToken	0xb5eef4df2e48fb41e6eae6778c14787baaa181f1

MUNDUS
SECURITY

Table of contents

MUNDUS
SECURITY

Findings summary

Storage findings

#	contract	storage issues initial check
2	ACLManager	found
5	EmissionManager	found
15	PullRewardsTransferStrategy	found
16	ReservesSetupHelper	found
21	Treasury-Controller	found

MUNDUS
SECURITY

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.	6
total		6

ID-2. ACLManager

issue #	issue type
1	EOA

1. EOA 0x0f6e98a756a40dd050dc78959f45559f98d3289d possesses EMERGENCY_ADMIN role.

ID-5. EmissionManager

issue #	issue type
1	EOA

1. _emissionAdmins, mapping(address => address) - EOAs

NOTE: EOAs are marked with ⚠.

reward	admin
0x642ce49f36f74fcc430f...	0x0f6e98a756a40dd050dc... ⚠

ID-15. PullRewardsTransferStrategy

issue #	issue type
1	EOA
2	EOA

1. rewardsAdmin = 0x0f6e98a756a40dd050dc78959f45559f98d3289d -- EOA
2. rewardsVault = 0x0f6e98a756a40dd050dc78959f45559f98d3289d -- EOA

ID-16. ReservesSetupHelper

issue #	issue type
1	EOA

1. _owner = 0x0f6e98a756a40dd050dc78959f45559f98d3289d -- EOA

ID-21. Treasury-Controller

issue #	issue type
1	EOA

1. _owner = 0x0f6e98a756a40dd050dc78959f45559f98d3289d -- 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.