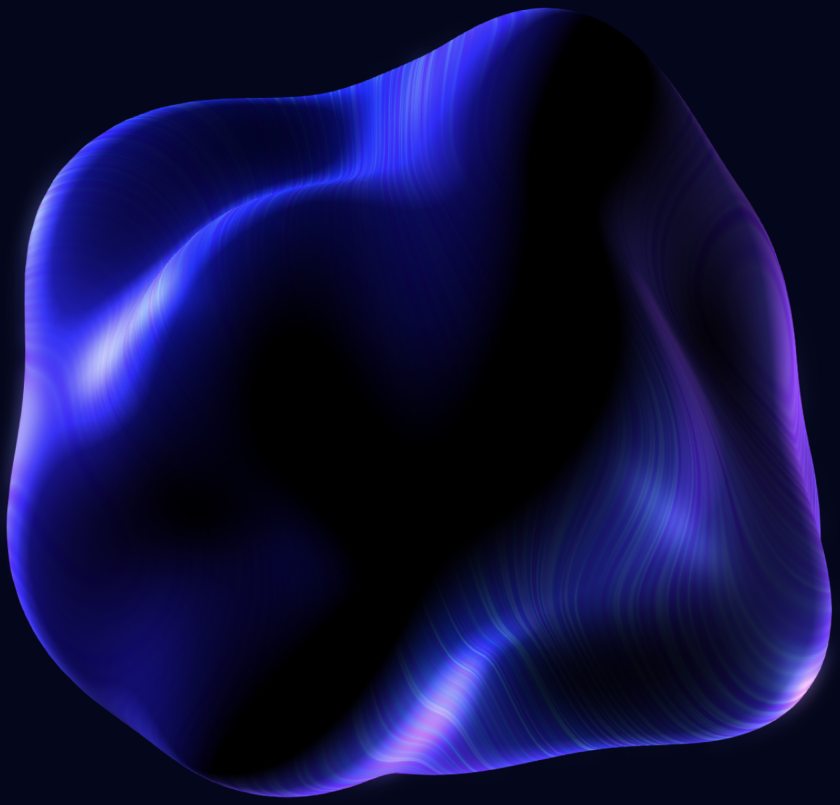
MUNDUS
SECURITY

Zerolend Deployment Check on Ethereum Mainnet



ZeroLend

MUNDUS
SECURITY

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

MUNDUS
SECURITY

Scope of work

#	contract	address
1	AaveOracle-mainnet-lrt	0x1cc993f2c8b6fbc43a9bafd2a44398e739733385
2	ACLManager-mainnet-lrt	0x749df84fd6de7c0a67db3827e5118259ed3abba5
3	EmissionManager	0x859c2ca97ead2742a0758bc9dd889e9d0e7e84e8
4	IncentivesProxy	0x5be89bb10e2234204a2607765714916ed95a73a2
5	IncentivesV2-Implementation	0x854138f891fe0a86270f6f153a06fbfabf69e0ad
6	ParaSwapLiquiditySwapAdapter	0x189cfdb4d7a08d926ca209d84a713c4c629645af
7	ParaSwapRepayAdapter	0x80ce5a187e477663fcfe99a108eefd9fbf0acc18
8	Pool-Implementation	0xff679e5b4178a2f74a56f0e2c0e1fa1c80579385
9	Pool-Proxy-mainnet-lrt	0x3bc3d34c32cc98bf098d832364df8a222bbab4c0
10	PoolAddressesProvider-mainnet-lrt	0xfd856e1a33225b86f70d686f9280435e3ff75fcf
11	PoolAddressesProviderRegistry	0x7503a8823b523629e28587317901ba4c055791eb
12	PoolConfigurator-Implementation	0x9c6f1367256be65ee744740c72ad80da5bc96ca6
13	PoolConfigurator-Proxy-mainnet-lrt	0x09edc8f101897aa693932c1966725e05d6d68b5f
14	PoolDataProvider-mainnet-lrt	0x47223d4ea966a93b2cc96ffb4d42c22651fadfcf
15	ReservesSetupHelper	0xc58715d0046bd873cedcc70fa3656ee2523e8011
16	ReserveStrategy-rateStrategyStableOne	0x81b3184a3b5d4612f2c26a53da8d99474b91b2d2
17	ReserveStrategy-rateStrategyStableTwo	0xa32eb787f2a3dc1f2c2da0e5d8cae7ff74e6fd32
18	ReserveStrategy-rateStrategyVolatileOne	0xcbdc0aed7cdf2472784068abef23a902cafabb98
19	Treasury-Controller	0x5300a1a15135ea4dc7ad5a167152c01efc9b192a
20	Treasury-Implementation	0x80f2c02224a2e548fc67c0bf705ebfa825dd5439
21	TreasuryProxy	0x464c71f6c2f760dda6093dcb91c24c39e5d6e18c

#	contract	address
22	UiIncentiveDataProviderV3	0x0a1198ddb5247a283f76077bb1e45e5858ee100b
23	UiPoolDataProviderV3	0xa6ea08d16d47fee408505fda73520ebefc68ef01
24	WalletBalanceProvider	0xa1e6bcdab01b9d7de83647d1bbd4113c6c2b4e0d
25	AToken-mainnet-lrt	0xb7ed499e7570ee7691eef4df9d708d258de2b512
26	DelegationAwareAToken-mainnet-lrt	0x4fcb7f18fa9255b52793dfd865d245bcec871468
27	WrappedTokenGatewayV3	0x6ea9d99c6653df987bdea11ffcd56dfb4b5d38b4
28	StableDebtToken-mainnet-lrt	0xe230cf9cee7b299f69778ef950a61de0de520ba7
29	BorrowLogic	0x8676e39b5d2f0d6e0d78a4208a0ccbc50504972e
30	BridgeLogic	0x3365d8691cd54313fa3df201bb33bd1ec37b9f9d
31	ConfiguratorLogic	0xb8634e0a320d0f4861062514a63b659e52a87e21
32	EModeLogic	0x78ad3d53045b6582841e2a1a688c52be2ca2a7a7
33	FlashLoanLogic	0x86b07c01b10545c7e093521cdeacf90d909db5a1
34	LiquidationLogic	0xbe0ab675a478a759eca580f0d6c9d399085547d8
35	PoolLogic	0xb2178109a414c3a869e5104283fcf1a18923d0b8
36	SupplyLogic	0x4db095bd39bde10a4b9be6ff63d98fceb2381fdc
37	DAI-AToken-mainnet-lrt	0x29a3a6af690942a3b7665bb2839a3f563c6f987b
38	DAI-StableDebtToken-mainnet-lrt	0x8569052157069ed81f603001596ee8ae1c85e049
39	DAI-VariableDebtToken-mainnet-lrt	0x0047cac82cf5fb36954de1b9d86d657915ab3b47
40	ezETH-AToken-mainnet-lrt	0x68fd75cf5a91f49effad0e857ef2e97e5d1f35e7
41	ezETH-StableDebtToken-mainnet-lrt	0x1e7f2afd1d534077656a0cfa7871358cb346f578
42	ezETH-VariableDebtToken-mainnet-lrt	0x27c1706ddd2467622ca63aaec03332127919a690
43	rsETH-AToken-mainnet-lrt	0xef4a41e692319ae4aa596314d282b3f2a3830bed
44	rsETH-StableDebtToken-mainnet-lrt	0x3af8bad4ca56afae60fa3a2f116cdea803c80fbc
45	rsETH-VariableDebtToken-mainnet-lrt	0xe4fe2d282dead5759199df364f3f419dfac17339

#	contract	address
46	USDC-AToken-mainnet-lrt	0xb2feb2c46305329a340e6188532f31fce9347a5c
47	USDC-StableDebtToken-mainnet-lrt	0x7fae822dc0a2ae436ec10b83ae5686c008fca718
48	USDC-VariableDebtToken-mainnet-lrt	0x227f86fbfccb5664403b62a5b6d4e0e593968275
49	USDT-AToken-mainnet-lrt	0x6c735966bc965bd4066c14fca3df443496ce14fb
50	USDT-StableDebtToken-mainnet-lrt	0x14b0f7edb2471350dee88b1c423e0df25c37b638
51	USDT-VariableDebtToken-mainnet-lrt	0xdaccf47046ae4fee3f9f3bcfe68696a95db6ccb7
52	VariableDebtToken-mainnet-lrt	0x5d50be703836c330fc2d147a631cdd7bb8d7171c
53	weETH-AToken-mainnet-lrt	0x84e55c6bc5b7e9505d87b3df6ceff7753e15a0c5
54	weETH-StableDebtToken-mainnet-lrt	0x4931dae3f4196499319l8d9e545d0f52cae0dbec
55	weETH-VariableDebtToken-mainnet-lrt	0x53c94fd63ef4001d45744c311d6bbe2171d4a11e
56	WETH-AToken-mainnet-lrt	0xfb932a75c5f69d03b0f6e59573fde6976af0d88c
57	WETH-StableDebtToken-mainnet-lrt	0x346623faf3cd1dbe9024c1d160cd40e6a90092ed
58	WETH-VariableDebtToken-mainnet-lrt	0x7ef98cd28902ce57b7aeec66dfb06b454cda1941
59	GnosisSafeProxy	0x4e88e72bd81c7ea394cb410296d99987c3a242fe
60	GnosisSafe	0xd9db270c1b5e3bd161e8c8503c55ceabee709552

MUNDUS
SECURITY

Table of contents

Findings summary

Storage findings

#	contract	storage issues initial check
2	ACLManager-mainnet-lrt	found
3	EmissionManager	found
6	ParaSwapLiquiditySwapAdapter	found
7	ParaSwapRepayAdapter	found
15	ReservesSetupHelper	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
2	EOA

1. EOA 0x0323acd6062b463c205fb2e76ca020ddae0d8e98 possesses EMERGENCY_ADMIN role.
2. EOA 0x9ad0395264c7c45b0486e5890cf794c2774c1540 possesses EMERGENCY_ADMIN role.

ID-3. EmissionManager

issue #	issue type
1	EOA

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

NOTE: EOAs are marked with ⚠.

reward	admin
0x3db28e471fa398bf2527...	0x0f6e98a756a40dd050dc... ⚠
0x420c440d4fce299f9c0c...	0x0f6e98a756a40dd050dc... ⚠
0x458de013d48bb1d34041...	0x0f6e98a756a40dd050dc... ⚠
0x30835d74a15be0e23bcf...	0x0f6e98a756a40dd050dc... ⚠

ID-6. ParaSwapLiquiditySwapAdapter

issue #	issue type
1	EOA

1. _owner = 0x0f6e98a756a40dd050dc78959f45559f98d3289d -- EOA

ID-7. ParaSwapRepayAdapter

issue #	issue type
1	EOA

1. _owner = 0x0f6e98a756a40dd050dc78959f45559f98d3289d -- EOA

ID-15. ReservesSetupHelper

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.