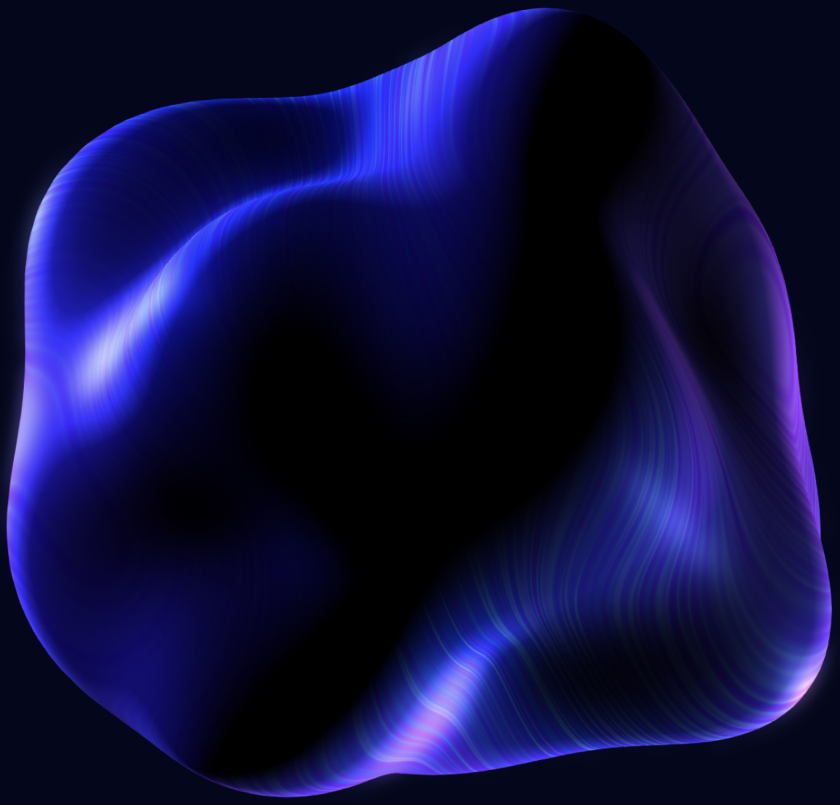
MUNDUS
SECURITY

Zerolend Deployment Check on Blast Network



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

MUNDUS
SECURITY

Scope of work

#	contract	address
1	Blast-Points-Receiver	0x53a3aa617afe3c12550a93ba6262430010037b04
2	ACLManager-blast	0x7503a8823b523629e28587317901ba4c055791eb
3	AToken-blast	0xa754b2f1535287957933db6e2aee2b2fe6f38588
4	AaveOracle-blast	0xbe0ab675a478a759eca580f0d6c9d399085547d8
5	Blast-AToken-blast	0x749df84fd6de7c0a67db3827e5118259ed3abba5
6	BlastAToken	0xcffe406e87ee9951696d910e63b0b22d7bc85401
7	DelegationAwareAToken-blast	0xcc8a5b5010c8a3832ecd2763e5b0e17811fbbd26
8	EmissionManager	0xfd856e1a33225b86f70d686f9280435e3ff75fcf
9	IncentivesProxy	0x94dc19a5bd17e84d90e63ff3fba9c3b76e5e4012
10	IncentivesV2-Implementation	0xb47d417f55080081c6fad95c3a470fe98a97e603
11	Pool-Implementation	0x3fc90e521397b251d4aaa1fbeac7cc32f25e78fa
12	Pool-Proxy-blast	0xa70b0f3c2470abbe104bdb3f3aaa9c7c54bea7a8
13	PoolAddressesProvider-blast	0xb0811a1fc9fb9972ee683ba04c32cb828bcf587b
14	PoolAddressesProviderRegistry	0xbbaef34d75e15c5d04a078fc2634245842eabdc7
15	PoolConfigurator-Implementation	0x844bd3eef0e454c6e273e2061e17308677e35fb4
16	PoolConfigurator-Proxy-blast	0x22d3cdb2fbd1528a0ebb047ec4de369098efcda1
17	PoolDataProvider-blast	0xc6df4dddbfacb866e78dcc01b813a41c15a08c10
18	PullRewardsTransferStrategy	0x72f7566116211cd4940cb3452df208c23297425a
19	ReserveStrategy-rateStrategyStableOne	0x854138f891fe0a86270f6f153a06fbfabf69e0ad
20	ReserveStrategy-rateStrategyStableTwo	0x0a8058203387c15a711204908ed9efed9f76e6a8
21	ReserveStrategy-rateStrategyVolatileOne	0x859c2ca97ead2742a0758bc9dd889e9d0e7e84e8
22	ReservesSetupHelper	0xc44827c51d00381ed4c52646aeab45b455d200eb

#	contract	address
23	StableDebtToken-blast	0x1cc993f2c8b6fbc43a9bafd2a44398e739733385
24	Treasury-Controller	0x89fec31dad373922879bd6279ccdc3666c5d1b7a
25	Treasury-Implementation	0x59423cceb710266520db98034ff62dd1e2090e10
26	TreasuryProxy	0x9698fdf843cbe4531610ac231b0047d9ffc13bc6
27	UiIncentiveDataProviderV3	0x66f3015534fae808773422e32b74f5732668dd5b
28	UiPoolDataProviderV3	0xe230cf9cee7b299f69778ef950a61de0de520ba7
29	VariableDebtToken-blast	0xd2a2a567674e85bedab9dcc402bcae6c4e0aabb8
30	WalletBalanceProvider	0x4fcb7f18fa9255b52793dfd865d245bcec871468
31	WrappedTokenGatewayV3	0xfadfb0bc400427663020887e7c8073d03a35dc3c
32	BlastLogic	0x1615ea4be9a29b62e59b58d02b7549d954f5b1d8
33	BorrowLogic	0x5e35d90db7118c2ae96a8de458401986879bb0ef
34	BridgeLogic	0xb0b0b1d3c0f9823c13d4e0481e86387baff452a2
35	ConfiguratorLogic	0xc3b6ddc1c9876a922754f1d01d18893c7956a74d
36	EModeLogic	0x7fab93af49ce663dbc2f94bc4def5c84d6605663
37	FlashLoanLogic	0x9660b39d0e38be0f7e09cc6c516bd335746262ee
38	LiquidationLogic	0xd85bbd487b957857d10d7d96f3a08f6bab55f7e3
39	PoolLogic	0x15785c5d383fa33339cf5d5720546c24313bc66d
40	SupplyLogic	0x5046c3c0d7a362709df433d5431d64973c7f08cb

MUNDUS
SECURITY

Table of contents

MUNDUS
SECURITY

Findings summary

Storage findings

#	contract	storage issues initial check
2	ACLManager-blast	found
8	EmissionManager	found
22	ReservesSetupHelper	found
24	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.	4
total		4

ID-2. ACLManager

issue #	issue type
1	EOA

1. EOA `0x0f6e98a756a40dd050dc78959f45559f98d3289d` possesses `POOL_ADMIN` role.

ID-8. EmissionManager

issue #	issue type
1	EOA

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

NOTE: EOAs are marked with ⚠.

reward	admin
0x81b3184a3b5d4612f2c2...	0x0f6e98a756a40dd050dc... ⚠
0xc2764d3ffbb6fbc3e1b1...	0x0f6e98a756a40dd050dc... ⚠
0x0a1198ddb5247a283f76...	0x0f6e98a756a40dd050dc... ⚠

ID-22. ReservesSetupHelper

issue #	issue type
1	EOA

1. `_owner = 0x0f6e98a756a40dd050dc78959f45559f98d3289d -- EOA`

MUNDUS
SECURITY

ID-24. 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.