HackenProof

SUMMARY REPORT

Kiichain SC DualDefense Audit

KiiChain

SMART CONTRACTS CODE LANGUAGE	REPORT CREATED
Go	19.06.2026
AUDIT DURATION	**PREPARED BY**
08 May 2026 - 08 Jun 2026	HackenProof Team

HackenProof | KiiChain

This report was prepared for the KiiChain DualDefense Audit

The report contains information about participants, in-scope targets as well as information about vulnerabilities found and fixed in the smart contracts code.

Approved by	HackenProof Team
Name	Kiichain SC DualDefense Audit
Type	Blockchain
Technology	Go
Timeline	08 May 2026 - 08 Jun 2026
Deployed contract / GitHub	Public

HackenProof | KiiChain

Table of Contests

HackenProof | KiiChain

OVERVIEW

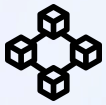
ABOUT AUDIT

BUDGET ALLOCATED	TOTAL REPORT SUBMITTED	SCOPE REVIEW COUNT
10 000 $	231	13072

ABOUT KIICHAIN

KiiChain is a blockchain project focused on stablecoins and real-world assets, aimed at supporting practical financial use cases. Its broader goal is to improve utility, liquidity, and accessibility for users, businesses, and developers, particularly in emerging markets.

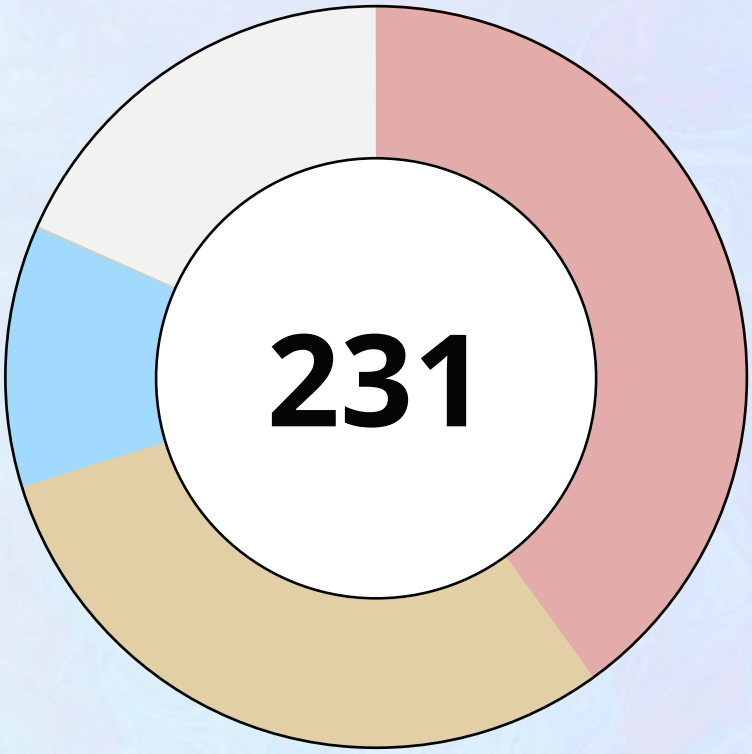
SCOPES AND TARGETS

Target	Type	Tech
https://github.com/KiiChain/kiichain/tree/f632e7faf979ceb6822be087585798e18db32a3b	 Blockchain	 Go

HackenProof | KiiChain

FINDINGS

VALID REPORTS STATISTICS STATISTICS



- Critical - 0
- High - 92
- Medium - 69
- Low - 26
- Informative - 42

SIGNAL-TO-NOISE RATIO

Displays the ratio of the Valid reports and Received reports. Valid reports include Informative, Triaged, Paid, Resolved, Disclosed statuses

FINDINGS LIST

Name	Severity	Submission date
KCNL1DDA-1 EVM Gas Refund Math Lets Users Consume Block Gas With Zero Net Fee	• High	08.05.2026
KCNL1DDA-32 Any unprivileged wasm contract drives ~853× SDK-gas undercharge of EVM compute via `wasmbinding/evm.HandleEthCall`, enabling sub-cent chain-halt DoS	• High	08.05.2026
KCNL1DDA-104 Feegrant Denomination Bypass via Post-Allowance Fee Conversion	• Medium	13.05.2026
KCNL1DDA-15 TWAP Overflow Panic in `CalculateTwaps` Causes Permanent Chain Halt via Validator-Submitted Extreme Exchange Rate	• Medium	08.05.2026

Name	Severity	Submission date
KCNL1DDA-164 Oracle Cross-Rate Threshold Bypass Allows Valid Votes to Panic EndBlocker and Halt the Chain	• Medium	22.05.2026
KCNL1DDA-80 Feeless Oracle Vote Attack	• Medium	10.05.2026
KCNL1DDA-9 Fee Abstraction Permanent Deactivation on Oracle Downtime	• Medium	08.05.2026
KCNL1DDA-2 Permanent Blockchain Halt via Uncaught Error in x/rewards BeginBlocker	• Medium	08.05.2026
KCNL1DDA-13 Reward Pool Exhaustion via Forced Minimum Release Logic in `x/rewards`	• Medium	08.05.2026
KCNL1DDA-47 Stale Oracle Prices Are Re-Snapshotted as Fresh TWAP Data, Allowing Near-Free Executed Transactions Through Fee Abstraction	• Medium	09.05.2026

Name	Severity	Submission date
KCNL1DDA-17 Validators Escape Slash Penalty Due to Mutated voteTargets Map in EndBlocker	• Medium	08.05.2026
KCNL1DDA-107 ClampPrice Symmetric 98.9% Fee Underpayment Window on All Fee-Abstracted Transactions After Fee-Token Market Crash	• Medium	14.05.2026
KCNL1DDA-153 ICA authz MsgExec bypasses host allowlist and EVM ante for MsgEthereumTx	• Medium	21.05.2026
KCNL1DDA-190 EIP-7702 delegated EOAs cannot self-revoke or send direct EVM transactions through KiiChain feeabstraction ante	• Medium	27.05.2026
KCNL1DDA-18 Unweighted Standard Deviation Allows Low-Power Validators to Inflate Oracle Reward Band by 3.7x	• Low	08.05.2026

Name	Severity	Submission date
KCNL1DDA-19 MsgVoteWeighted and Nested Authz Bypass Governance Vote Stake Requirement	• Low	08.05.2026
KCNL1DDA-78 Authz-Wrapped Expedited Governance Proposals Bypass the Antehandler Whitelist	• Low	09.05.2026
KCNL1DDA-4 Resource Exhaustion (DoS) in Oracle Precompile via Gas Undercharging	• Low	08.05.2026
KCNL1DDA-27 TWAP Price Snapshot Silently Overwritten When Two Blocks Share Same Unix Second	• Low	08.05.2026
KCNL1DDA-25 MintTo Not Gated by Capability Flag -- Asymmetric with BurnFrom and ForceTransfer	• Low	08.05.2026

HackenProof | KiiChain

PAYMENT STATISTICS

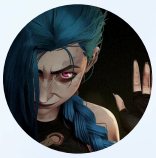
REWARDS TO SECURITY RESEARCHERS

The following researchers submitted unique valid findings during the DualDefense audit period and contributed to the security of the protocol

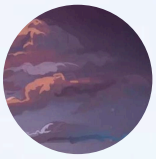
SECURITY RESEARCHERS

TOP HACKERS

The following researchers submitted unique valid findings during the DualDefense audit period and contributed to the security of the protocol

Researcher	Submissions	Rank
 itzdaglitch	2	18
 MantisTheAlpha	2	12

Researcher	Submissions	Rank
 ahmad044	3	13
 0x0001	13	5
 HiteshRajpurohit	6	4
 0xYAHYA	3	13
 Ramirez911	7	3
 alhibb01	5	6
 nooz0x	3	54
 pengus101	1	49

Researcher	Submissions	Rank
 zpano	5	8
 0xangky	1	72

CONCLUSION

ABOUT DUALDEFENSE

The audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract.

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 security of smart contracts.

TECHNICAL DISCLAIMER

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