



HackenProof

SUMMARY REPORT

Somnia Audit Contest



SMART CONTRACTS CODE LANGUAGE

C++

REPORT CREATED

29.10.2025

AUDIT DURATION

06.08.25-20.09.25

PREPARED BY

HackenProof team

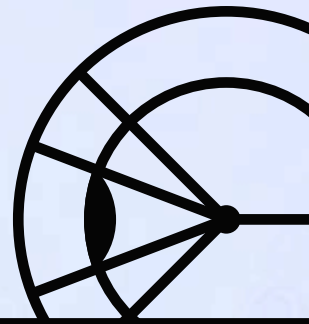
HackenProof Crowdsourced Audit is your solution to maximize the cybersecurity level with involvement of over 30k of the most skilled and experienced community researchers in the industry

Approved by	HackenProof team
Name	Somnia Audit Contest
Type	L1
Technology	C++
Timeline	06.08.25-20.09.25
Deployed contract / GitHub	Public

Table of Contents

Overview	4
About audit	4
About Somnia	4
Scopes and targets	5
Payment statistics	6
Rewards distribution	6
Findings	7
Valid reports statistics	7
Signal-to-noise ratio	7
Findings list	8-12
Security researchers	13
Top hackers	13
Conclusion	14
About Somnia	14
Technical disclaimer	14

OVERVIEW



ABOUT AUDIT

BUDGET
ALLOCATED

\$300 000

TOTAL REPORT
SUBMITTED

275

SCOPE REVIEW
COUNT

14517

ABOUT SOMNIA

Somnia is a high-performance, cost-efficient EVM-compatible Layer 1 blockchain capable of processing over 1,000,000 transactions per second (TPS) with sub-second finality. It is suitable for serving millions of users and building real-time mass-consumer applications like games, social applications, metaverses, and more, all fully on-chain.

SCOPES AND TARGETS

Target

Type

Tech

<https://github.com/hackenproof-public/somnia>



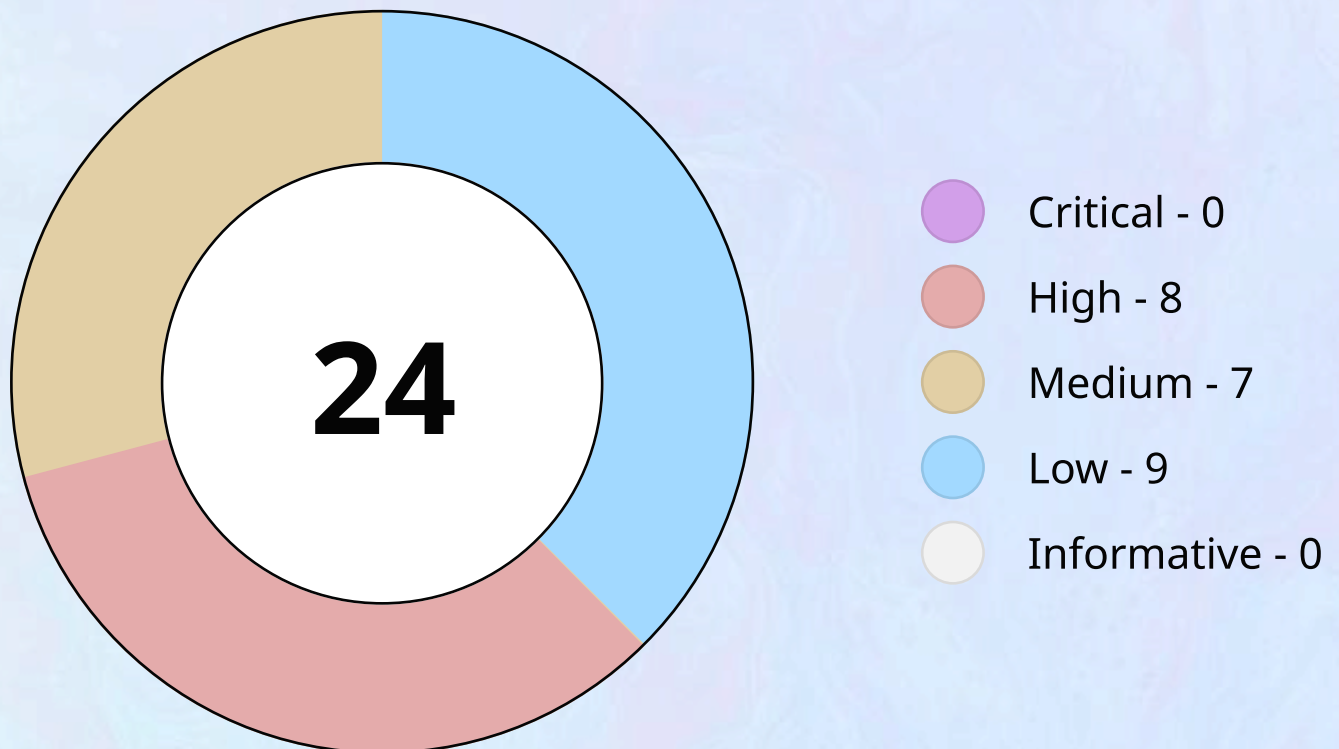
L1



C++

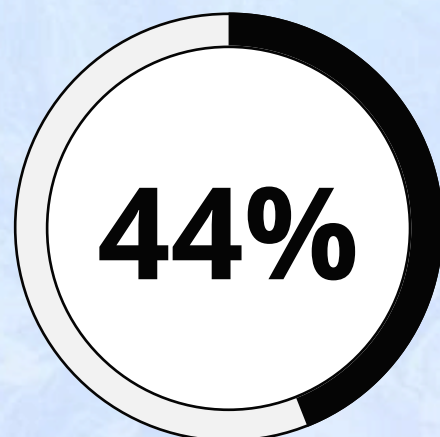
FINDINGS

VALID REPORTS STATISTICS



SIGNAL-TO-NOISE RATIO

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



FINDINGS LIST

	Name	Severity	Submission date
	SOMNIAAC-53 <u>LeaderViewChangeMessage is not properly checked, and malicious request payloads can be inserted, leading to total network shutdown with fork</u>	• High	21.08.2025
	SOMNIAAC-65 <u>Validators can pre-prepare request batches for views that have not yet started, which can lead to colliding request batches</u>	• High	25.08.2025
	SOMNIAAC-69 <u>data_chain_block_resources is not properly validated when a validator receives a data chain block, which leads to a RELEASE_ASSERT during decompression</u>	• High	27.08.2025
	SOMNIAAC-112 <u>Unbounded data chain creation lead to memory exhaustion and chain halt</u>	• High	08.09.2025

	Name	Severity	Submission date
	SOMNIAAC-132 <u>Somnia - Node Crash via Null Pointer Dereference</u>	• High	10.09.2025
	SOMNIAAC-144 <u>SendMempoolTransaction RequestMessage can contain a malicious transaction that crashes a node</u>	• High	12.09.2025
	SOMNIAAC-225 <u>Somnia - Node Crash via Bitset Capacity Violation</u>	• High	18.09.2025
	SOMNIAAC-243 <u>A malicious PBFT node can spoof the signature of another validator's Prepare message</u>	• High	19.09.2025
	SOMNIAAC-110 <u>Lack of throttling protection in data network lead to CPU/memory waste and DDoS risk</u>	• Medium	08.09.2025
	SOMNIAAC-126 <u>Consensus Liveness Failure via Mempool Exhaustion from Unvalidated Transactions</u>	• Medium	10.09.2025

Name

Severity

Submission date



SOMNIAAC-127

Memory Exhaustion via
Unbounded Storage of
Orphaned Data Chain Blocks

• Medium

10.09.2025



SOMNIAAC-131

Somnia - Peer
Impersonation Attack via
Challenge Replay

• Medium

10.09.2025



SOMNIAAC-163

DoS attack due memory leak
in
InFlightTransactionTracker::i
n_flight_accounts

• Medium

15.09.2025



SOMNIAAC-177

Node liveness halt via
spoofed bootstrap status
messages

• Medium

16.09.2025



SOMNIAAC-180

Non-existent
ConsensusFinishedNetwork
Message Stuck in
inflight_protocol_requests
forever Cause Node
Resource Exhaustion and
DOS

• Medium

17.09.2025

Name

Severity

Submission date



SOMNIAAC-42

Somnia Accepts Non-Canonical v Values in Typed Transactions, Enabling Transaction Malleability

• Low

17.08.2025



SOMNIAAC-66

Unbounded growth of half-open peer connections can exhaust slots and denying access to RPC/API/P2P services.

• Low

25.08.2025



SOMNIAAC-68

Unbounded API Subscriptions Allow Resource Exhaustion

• Low

27.08.2025



SOMNIAAC-145

When a data chain block is received, there is no proper validation of the block number

• Low

12.09.2025



SOMNIAAC-149

Liveness messages can be spoofed because the sender is not validated

• Low

13.09.2025



SOMNIAAC-160

ECDSA verify is malleability-tolerant without low-S enforcement

• Low

15.09.2025

Name

Severity

Submission date



SOMNIAAC-161

WebSocket client frames are never masked

• Low

15.09.2025



SOMNIAAC-162

WebSocket handshake uses a fixed client key

• Low

15.09.2025



SOMNIAAC-168

DoS attack due to memory leak in MempoolTransactionQueue::sender_accounts

• Low

15.09.2025

SECURITY RESEARCHERS

TOP HACKERS

Researcher	Total findings	Payouts	Place
 @Blockian Blockian	8	\$31,898.72	1
 @Schnilch	11	\$31,044.29	2
 @dontonka	8	\$17,943.03	3
 @fromeo-016	19	\$10,253.16	4
 @destin029 Ehiosun Destiny Friday	16	\$10,253.16	5

CONCLUSION

ABOUT SOMNIA

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.