SALUS SECURITY

SEP 2024

CODE SECURITY ASSESSMENT

NUBIT

Overview

Project Summary

- Name: Nubit - Native Token
- Platform: Nubit Chain
- Language: Go
- Repository:
    - https://github.com/RiemaLabs/cosmos-sdk
- Audit Range: See Appendix - 1

Project Dashboard

Application Summary

Name	Nubit - Native Token
Version	v2
Type	Solidity
Dates	Sep 15 2024
Logs	Sep 14 2024; Sep 15 2024

Vulnerability Summary

Total High-Severity issues	0
Total Medium-Severity issues	0
Total Low-Severity issues	1
Total informational issues	0
Total	1

Contact

E-mail: support@salusec.io

SALUS

Risk Level Description

High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for clients' reputations or serious financial implications for clients and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental to the client's reputation if exploited, or is reasonably likely to lead to a moderate financial impact.
Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
Informational	The issue does not pose an immediate risk, but is relevant to security best practices or defense in depth.

SALUS

Content

SALUS

Introduction

1.1 About SALUS

At Salus Security, we are in the business of trust.

We are dedicated to tackling the toughest security challenges facing the industry today. By building foundational trust in technology and infrastructure through security, we help clients to lead their respective industries and unlock their full Web3 potential.

Our team of security experts employ industry-leading proof-of-concept (PoC) methodology for demonstrating smart contract vulnerabilities, coupled with advanced red teaming capabilities and a stereoscopic vulnerability detection service, to deliver comprehensive security assessments that allow clients to stay ahead of the curve.

In addition to smart contract audits and red teaming, our Rapid Detection Service for smart contracts aims to make security accessible to all. This high calibre, yet cost-efficient, security tool has been designed to support a wide range of business needs including investment due diligence, security and code quality assessments, and code optimisation.

We are reachable on Telegram (https://t.me/salusec), Twitter (https://twitter.com/salus_sec), or Email (support@salusec.io).

1.2 Audit Breakdown

The objective was to evaluate the repository for security-related issues, code quality, and adherence to specifications and best practices. Possible issues we looked for included (but are not limited to):

- Risky external calls
- Integer overflow/underflow
- Transaction-ordering dependence
- Timestamp dependence
- Access control
- Call stack limits and mishandled exceptions
- Number rounding errors
- Centralization of power
- Logical oversights and denial of service
- Business logic specification
- Code clones, functionality duplication

1.3 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release and does not give any warranties on finding all possible security issues with the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues.

SALUS

Findings

2.1 Summary of Findings

ID	Title	Severity	Category	Status
1	Third-party dependencies	Low	Dependency	Acknowledged

SALUS

2.2 Notable Findings

Significant flaws that impact system confidentiality, integrity, or availability are listed below.

1. Third-party dependencies

Severity: Low	Category: Dependency
Target: - All	

Description

Nubit's native token relies on the third-party library Cosmos-sdk. This audit treats third-party entities as a black box and assumes they function correctly. However, in reality, third-party components may be compromised, potentially rendering the Nubit chain unusable or vulnerable to damage.

Recommendation

We understand that the business logic requires interaction with the third parties. We encourage the team to regularly monitor the statuses of third parties to reduce the impacts when they are not functioning properly.

Status

This issue has been acknowledged by the team.

SALUS

2.3 Informational Findings

No informational issues were found.

SALUS

Appendix

Appendix 1 - Files in Scope

This audit covered the files in commit be8e4d0.

Appendix 2 - About Target Project

Nubit is a Cosmos-compatible chain built on the Cosmos-SDK. This audit covers only the chain infrastructure and does not include modules such as the consensus protocol.

The primary objective is to ensure that the underlying infrastructure operates securely and safely within its expected parameters.

SALUS