RESPONSIBLE DISCLOSURE

Nois Network

nois-proxy Contract

Prepared by SCV-Security
On 15th December 2023

Introduction

Nois is a Proof of Stake blockchain protocol that allows developers to obtain unbiased and cost efficient randomness via IBC. Nois provides a decentralized solution based on Drand that brings randomness beacon to Dapps and other implementations for Web3.

During an internal security review of a specific Dapp contract functionality involving nois-proxy CosmWasm contract SCV team has identified a notable aspect that has caught our attention. It's important to note that the SCV-Security did not conduct a comprehensive audit of these contracts or additional components of Nois Network.

The nois-proxy is like a messenger between different apps, hanging out on the app chain. It's like the go-to when a consumer app needs some randomness. When these apps ask for randomness, the nois-proxy takes their requests and sends them over to the Nois chain using IBC. Once the Nois chain has the randomness ready, it relays back to the requester.

About the Vulnerability

The nois-proxy can be instantiated with a custom attribute called *allowlist_enabled* which defines allowed addresses to request randomness.

Since $NOIS tokens are used to pay for the fee when requesting randomness the allowlist is often required between implementations to avoid the fee-exhaustion and consequently funds abuse.

The *allowlist_enabled* is an Option due to compatibility with older versions of the proxy contract. If set to *None* it means it's disabled. From instances running version 0.13.5 onwards, the value is always set to *Some(..)*.

In summary, it has these 3 cases:

```
allowlist_enabled == None => disabled
allowlist_enabled == Some(false) => disabled
allowlist_enabled == Some(true) => enabled
```

The vulnerability arises in the third case when the *allowlist_enabled* is set to be True. This is due the fact that the execute_update_allowlist function is

permissionless allowing an attacker to prevent a contract from requesting randomness by removing them from the allowlist and draining (fee-exhaustion) funds that are held by the proxy by adding addresses to the allowlist.

Instead permissionless, the function should be asserting the contract manager config as seen here.

The impact risk if this issue is exploited heavily depends on each case and their implementation specifics.

Technical Details

In order to reproduce the issue, the following test (Gist) case can be used

Recommendations

It is advised to migrate the nois-proxy contract to the latest version containing the mitigation by the Nois team at v0.15.4. Once upgraded, the vulnerability will be effectively patched.

Special Thanks

On behalf the SCV team, we would like to thank individuals and teams that assisted us in this disclosure and directly collaborated:

- **SCV-Security Auditors team**, The entire SCV-Security technical team and the original contributor who identified and reported this vulnerability.
- **Nois Team**, especially Simon Warta, for acknowledging the vulnerability promptly and providing further context and detailed discussions.

Timeline

07th December *2023* – Issue identified.

08th December *2023*– Initial contact with Nois and issue acknowledgment.

09th December *2023*– Remediations.

10th - 14th December *2023* – Fetching affected and exposed teams.

15th December – v0.15.4 Released.