Audit Report

Dymension Point 1D Stream 6: RollApp White-box Pentest

v1.1

August 13, 2024

Table of Contents

License

Disclaimer

THE CONTENT OF THIS AUDIT REPORT IS PROVIDED “AS IS”, WITHOUT REPRESENTATIONS AND WARRANTIES OF ANY KIND.

THE AUTHOR AND HIS EMPLOYER DISCLAIM ANY LIABILITY FOR DAMAGE ARISING OUT OF, OR IN CONNECTION WITH, THIS AUDIT REPORT.

THIS AUDIT REPORT WAS PREPARED EXCLUSIVELY FOR AND IN THE INTEREST OF THE CLIENT AND SHALL NOT CONSTRUE ANY LEGAL RELATIONSHIP TOWARDS THIRD PARTIES. IN PARTICULAR, THE AUTHOR AND HIS EMPLOYER UNDERTAKE NO LIABILITY OR RESPONSIBILITY TOWARDS THIRD PARTIES AND PROVIDE NO WARRANTIES REGARDING THE FACTUAL ACCURACY OR COMPLETENESS OF THE AUDIT REPORT.

FOR THE AVOIDANCE OF DOUBT, NOTHING CONTAINED IN THIS AUDIT REPORT SHALL BE CONSTRUED TO IMPOSE ADDITIONAL OBLIGATIONS ON COMPANY, INCLUDING WITHOUT LIMITATION WARRANTIES OR LIABILITIES.

This audit has been performed by

Oak Security GmbH

https://oaksecurity.io/
info@oaksecurity.io

Introduction

Purpose of This Report

Oak Security has been engaged by Dymension Technologies Ltd to perform a white-box penetration test of a Dymension RollApp setup.

The objectives of the penetration test are as follows:

1. Determine the correct functioning of the setup, in accordance with the project specification.

2. Determine possible vulnerabilities, which could be exploited by an attacker.

3. Determine bugs in the deployed software, which might lead to unexpected behavior.

4. Analyze whether best practices have been applied for the infrastructure.

5. Make recommendations to improve the setup.

This report represents a summary of the findings.

As with any penetration test, there is a limit to which vulnerabilities can be found, and unexpected behavior may still be possible. The author of this report does not guarantee complete coverage (see disclaimer).

Setup Submitted for the Penetration Test

The client provided the private and public IP addresses of 8 different nodes:

- 1 RollApp node (not publicly reachable)
- 2 Sentry nodes
- 1 Grafana node
- 4 RPC nodes

Moreover, access to the source code of the software was provided in the following repositories:

Repository	https://github.com/dymensionxyz/roller
Commit	`1ca9f559f673fcdcfce29762696ae4f60722e79d`

Repository	https://github.com/dymensionxyz/rollapp-evm
Commit	3fbc166d19b29c0baa23b6fc64a19ce3cfcc1cad

Repository	https://github.com/dymensionxyz/dymension
Commit	d447bab6870962753a597cc48e0df63f6330120e

Methodology

The penetration test has been performed in the following steps:

1. Gaining an understanding of the system’s intended purpose by reading the available documentation.
2. Enumerating the environment with various tools.
3. Manual exploration and analysis of all exposed attack surfaces.
4. Manual line-by-line analysis of selected parts of the source code for security vulnerabilities where applicable.
5. Report preparation.

Functionality Overview

Dymension allows anyone to easily deploy RollApps, which are IBC-enabled app-chains.

How to Read This Report

This report classifies the issues found into the following severity categories:

Severity	Description
Critical	A serious and exploitable vulnerability that can lead to loss of funds, unrecoverable locked funds, or catastrophic denial of service.
Major	A vulnerability or bug that can affect the correct functioning of the system, lead to incorrect states or denial of service.
Minor	A violation of common best practices or incorrect usage of primitives, which may not currently have a major impact on security, but may do so in the future or introduce inefficiencies.
Informational	Comments and recommendations of design decisions or potential optimizations, that are not relevant to security. Their application may improve aspects, such as user experience or readability, but is not strictly necessary. This category may also include opinionated recommendations that the project team might not share.

The status of an issue can be one of the following: **Pending, Acknowledged**, or **Resolved**.

Note that penetration tests are an important step to improving the security of setups and can find many issues. However, auditing complex setups has its limits and a remaining risk is present (see disclaimer).

Summary of Findings

No	Description	Severity	Status
1	Expensive RPC methods are allowed	Minor	Acknowledged
2	Tendermint RPC API exposes private IP address	Informational	Acknowledged
3	Broken links in the Dymension EVM RollApp documentation	Informational	Acknowledged
4	Usage of deprecated functionality	Informational	Partially Resolved
5	Multiple subprocesses launched directly on the OS	Informational	Acknowledged

Enumeration

Architecture

The RollApp host itself was not directly reachable over the internet and only had a private IP within AWS. There were two sentry hosts that are publicly reachable and had a private IP in the same subnet as the RollApp host. Moreover, the details of 4 RPC hosts were provided, which were all publicly available and also had a private IP address in the same subnet.

Sentry hosts

A network scan of both hosts showed that only port 26656 was open. The setup therefore followed best practices and did not expose any unnecessary ports (for instance direct SSH access to the instances).

RPC hosts

The RPC hosts exposed the ports 8545 and 8546. Interacting with these ports showed that port 8545 is the HTTP JSON RPC port, whereas port 8546 is the WebSocket JSON RPC port. Moreover, port 26657 (Tendermint RPC with various endpoints) is exposed.

The JSON RPC API supports different endpoints that can be queried, for instance:

```
curl --header 'Content-Type: application/json' \
--data-raw '{
    "jsonrpc": "2.0",
    "method": "txpool_status",
    "params": [],
    "id": 1
}' http://3.76.181.197:8545
{"jsonrpc":"2.0","id":1,"result":{"pending":"0x0","queued":"0x0"}
```

One concern when exposing these endpoints to the internet are the methods in the admin namespace. Querying these methods returns an error:

```
curl --header 'Content-Type: application/json' \

--data-raw '{

    "jsonrpc": "2.0",

    "method": "admin_addPeer",

    "params": ["http://127.0.0.1"],

    "id": 1

}' http://3.76.181.197:8545
```

```
{"jsonrpc":"2.0","id":1,"error":{"code":-32601,"message":"the
method admin_addPeer does not exist/is not available"}}
```

The reason seems to be that EVMOS currently does not support the admin namespace. If this is changed at some point in the future, it is recommended to ensure that the methods are still not callable.

Initial Assessment

The evaluated systems followed all recommended best practices. Only the necessary ports were exposed, which limits the attack surface significantly. Moreover, the RollApp host is not directly reachable and there are sentry hosts in front of it.

While direct connections to the hosts are therefore not possible, it should be noted that another possible attack path involves the accounts that can change the network configuration or launch new hosts within the environment of the cloud provider (in this case AWS): If an attacker manages to compromise such an account (for instance via phishing), they can circumvent most protections and attack the hosts directly. It is therefore strongly recommended to implement rigorous processes (including MFA, limited access for only a few users, etc...) for these accounts.

Besides the mentioned security benefits of the architecture, it can also be helpful for the mitigation of DDoS attacks, as the sentry hosts can be scaled on demand if needed.

Detailed Findings

1. Expensive RPC methods are allowed

Severity: Minor

The analyzed RPC endpoints support all methods that are exposed by EVMOS. Among those, some methods may be problematic in terms of resource usage, for example:

- `debug_traceTransaction`: This method can be used to rerun and trace a prior transaction. Moreover, a trace configuration can be provided where memory capture can be enabled and a custom JavaScript expression can be supplied as the tracer.
- `debug_traceBlockByNumber`: Similar to `debug_traceTransaction`, but for a whole block.
- `txpool_content`: Lists all transactions that are currently pending.
- `txpool_inspect`: Similarly to `txpool_content`, but in text format.

The invocation of these methods can consume a lot of resources on the RPC server. An attacker might abuse this to overload the servers and perform (D)DoS attacks.

Recommendation

We recommend disabling the methods or requiring authentication for them (potentially with a credit system). For instance, some node providers take the resource usage into account and charge 3.5x - 25x more for these calls compared to other methods.

Status: Acknowledged

2. Tendermint RPC API exposes private IP address

Severity: Informational

The Tendermint RPC API can be used to get the private IP of a node via the `moniker` field:

```
curl http://52.29.63.91:26657/status
```

```
{"jsonrpc":"2.0","result":{"node_info":{"protocol_version":{"p2p":
"8","block":"11","app":"0"},"id":"002408011220944cd0e92a4060e0e79b
9a0ad58b3fd7a1e92c22db5b1623b7647754f23e3d92","listen_addr":"/ip4/
0.0.0.0/tcp/26656","network":"vaptra_2145170-1","version":"\u003cv
ersion\u003e","channels":"01","moniker":"ip-10-201-0-197","other":{
"tx_index":"on","rpc_address":"tcp://127.0.0.1:26657"}},"sync_info
":{"latest_block_hash":"E3B0C44298FC1C149AFBF4C8996FB92427AE41E464
9B934CA495991B7852B855","latest_app_hash":"E03886591492A5D62CD1164
2A294D9F08A82F0ADBA39EC0A057E9D0AA028E871","latest_block_height":"
34852","latest_block_time":"2024-03-16T19:45:02.643255719Z","earli
est_block_hash":"","earliest_app_hash":"","earliest_block_height":
"0","earliest_block_time":"0001-01-01T00:00:00Z","catching_up":fal
se},"validator_info":{"address":"25E427B4DE03FEBFAEEEB73EB7942FAE5
ABC3E03","pub_key":{"type":"tendermint/PubKeyEd25519","value":"yc/
TFWU3L8xfmxqVJvpoJfGQYOR7uG9Aqj3DSKBWTNo="},"voting_power":"1"}},"
id":-1}
```

The same information is also exposed via the `net_info` endpoint.

While this cannot be exploited, it is generally recommended to expose as little information as possible about the internal network structure.

Recommendation

We recommend using a different, more generic moniker.

Status: Acknowledged

3. Broken links in the Dymension EVM RollApp documentation

Severity: Informational

It has been noticed that the documentation describing the Dymension EVM RollApp contains references to links that lead to non-existent pages. This may be problematic for new users using the platform.

These are:

- Link in “Quick guide” section,
- Link in “Run local dymension hub node” section.

Recommendation

We suggest updating the links to point to expected resources on the Dymension documentation site.

Status: Acknowledged

4. Usage of deprecated functionality

Severity: Informational

It has been observed that the codebase contains calls to the deprecated functions. Namely, the `rand.Seed` function from the `math` module is used to set up the RNG. The `rand.Seed` has been deemed deprecated. The code that is using such functionalities can be found in the `roller/cmd/config/init/flags.go` and `roller/data_layer/celestia/generate_namespace_id.go` files.

Recommendation

We recommended restraining from using deprecated functionalities. The used RNG should be cryptographically secure and set up with up-to-date API.

Status: Partially Resolved

Some usages of rand.seed were replaced (e.g. in `roller/cmd/config/init/flags.go`), some remain (e.g. in `roller/data_layer/celestia/generate_namespace_id.go`).

5. Multiple subprocesses launched directly on the OS

Severity: Informational

It was observed that the codebase utilizes an `os/exec` module to run commands directly within the OS command line interface. Such calls could be susceptible to a Command Injection attack. Although, currently, the commands executed do not seem to take the input from users directly, it is still a best practice to avoid such an approach to multithreading. Furthermore, should an administrator responsible for configuring the system make a mistake, it increases the attack surface of the whole project.

Recommendation

We recommend ensuring that directly interacting with the OS command line interface is done only when necessary. In every other case - it should be avoided.

Status: Acknowledged