Audit Report

Apollo DAO 3

v1.0

January 17, 2023

Table of Contents

License

Disclaimer

This audit has been performed by

Oak Security

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

Introduction

Purpose of This Report

Oak Security has been engaged by Apollo DAO to perform a security audit of the Apollo DAO smart contracts.

The objectives of the audit are as follows:

1. Determine the correct functioning of the protocol, in accordance with the project specification.
2. Determine possible vulnerabilities, which could be exploited by an attacker.
3. Determine smart contract bugs, which might lead to unexpected behavior.
4. Analyze whether best practices have been applied during development.
5. Make recommendations to improve code safety and readability.

This report represents a summary of the findings.

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

Codebase Submitted for the Audit

The audit has been performed on the following GitHub repositories:

https://github.com/apollodao/cw-vault-token
Commit Hash: `d04ff1d6f4088b9d734f4190fb7023e22e72a8d8`

https://github.com/apollodao/cw-dex
Commit Hash: `de7394fdbc74a3401f4227f81389413991b309e3`

https://github.com/apollodao/osmosis-liquidity-helper
Commit Hash: `2bacac4a23a7ace472fef153190db311c11ad082`

https://github.com/apollodao/astroport-liquidity-helper
Commit Hash: `0eadc100d0894d3a4dac48392b1097065949691a`

https://github.com/apollodao/cw-dex-router
Commit Hash: `1db8457c7e7bb1dd093c086d8ef73e7105703343`

https://github.com/apollodao/apollo-utils
Commit Hash: `dd3da52653d3dc350b20b46f363ebcfdcd64aa27`

https://github.com/apollodao/apollo-vaults
Commit Hash: `65a8f2bbbd60930e1d77d215f9eb6adb5360cdb7`

Methodology

The audit has been performed in the following steps:

1. Gaining an understanding of the code base's intended purpose by reading the available documentation.
2. Automated source code and dependency analysis.
3. Manual line by line analysis of the source code for security vulnerabilities and use of best practice guidelines, including but not limited to:
    a. Race condition analysis
    b. Under-/overflow issues
    c. Key management vulnerabilities
4. Report preparation

Functionality Overview

This audit covers the functionality associated with Apollo DAO's vault contracts, vault token contract, CosmWasm DEX abstractions, liquidity helper contracts, and accompanying utility functions.

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 audits are an important step to improving the security of smart contracts and can find many issues. However, auditing complex codebases has its limits and a remaining risk is present (see disclaimer).

Users of the system should exercise caution. In order to help with the evaluation of the remaining risk, we provide a measure of the following key indicators: **code complexity**, **code readability**, **level of documentation**, and **test coverage**. We include a table with these criteria below.

Note that high complexity or low test coverage does not necessarily equate to a higher risk, although certain bugs are more easily detected in unit testing than in a security audit and vice versa.

Code Quality Criteria

The auditor team assesses the codebase's code quality criteria as follows:

Criteria	Status	Comment
Code complexity	Medium	-
Code readability and clarity	Medium-High	-
Level of documentation	Low-Medium	Lack of architectural and protocol documentation. Some of the repositories do not include inline function documentation.
Test coverage	Low	Some of the repositories do not have tests and others contain failing tests either at compile time or during execution.

Summary of Findings

No	Description	Severity	Status
1	Users will receive incorrect amount of LP tokens	Critical	Resolved
2	Balanced liquidity provision into constant product pool will fail	Major	Resolved
3	No validation of `min_out` for double sided liquidity provision	Major	Resolved
4	Insufficient validation of swap paths	Minor	Resolved
5	Insufficient validation of vault configuration	Minor	Resolved
6	Basket liquidation fails if no path is found for offer asset	Minor	Resolved
7	Lack of Osmosis Vault parameter validation	Informational	Resolved
8	Use of magic numbers throughout the codebase	Informational	Acknowledged
9	Additional funds sent to the contract are lost	Informational	Resolved
10	“Migrate only if newer” pattern not followed	Informational	Resolved
11	Unimplemented query entrypoint in liquidity helper causes panic	Informational	Resolved
12	Remove duplicate query functions	Informational	Acknowledged
13	Redundant asset validation	Informational	Resolved
14	Lack of clear function on admin two-step transfer mechanism	Informational	Resolved
15	Inconsistent usage of generic error	Informational	Resolved
16	Outdated dependencies	Informational	Resolved

Detailed Findings

1. Users will receive incorrect amount of LP tokens

Severity: Critical

The `execute_balancing_provide_liquidity` function in `osmosis-liquidity-helper/src/contract.rs:78` allows users to provide either a single asset or a pair of assets to a pool. In the case that a user provides multiple assets, the contract first performs a double-sided liquidity provision followed by a single-sided provision for any left over assets.

However, the LP tokens minted during the double sided liquidity provision are never transferred to the recipient. The LP tokens received from the initial liquidity provision that will be returned in response to the message in line `122` will never get recorded because the `ReturnLpTokens` callback was not called with the contract's initial `lp_token_balance`. The result will be that the caller will only receive LP tokens for the second liquidity provision.

Recommendation

We recommend adding a `ReturnLpTokens` callback to the else condition in `osmosis-liquidity-helper/src/contract.rs:115`. This will ensure that both tranches of LP tokens are returned to the recipient.

Status: Resolved

2. Balanced liquidity provision into constant product pool will fail

Severity: Major

When a user performs a balanced liquidity provision into a constant product pool in `astroport-liquidity-helper/src/contract.rs:90`, the contract first swaps any tokens to ensure the ratio remains constant and then supplies the tokens into the pool. Subsequently, the contract returns the received LP tokens to the recipient using the callback function `ReturnLpTokens`.

During execution of each message the contract will transfer the recently minted LP tokens from itself to the recipient. However, the callback function is called twice, first in `astroport-liquidity-helper/src/contract.rs:185-190` and then again in `250-255`.

The `ReturnLpTokens` callback that is defined in lines `185-190` will be executed before the liquidity is provisioned and the contract's balance changes. This will cause `return_amount` in line `274` to be `0`. When the function attempts to transfer a zero amount the CW20 transfer

function will return an error and revert the transaction. This will effectively block the `execute_balancing_provide_liquidity` function.

Recommendation

We recommend only executing callback messages a single time and removing the creation of the message in `astroport-liquidity-helper/src/contract.rs:185-190`.

Status: Resolved

3. No validation of `min_out` for double sided liquidity provision

Severity: Major

When providing liquidity in the `execute_balancing_provide_liquidity` function in `osmosis-liquidity-helper/src/contract.rs:78`, users are able to specify the `min_out` value which defines the minimum amount of LP tokens they want to receive when providing liquidity.

In the case that a user provides multiple assets to a pool, the amount of LP tokens minted is never checked to ensure it is greater than the value `min_out`. This means users may in fact receive fewer LP tokens than expected.

Recommendation

We recommend adding an additional check to the contract that ensures total LP tokens received are greater or equal to `min_out` in function `execute_balancing_provide_liquidity`.

Status: Resolved

4. Insufficient validation of swap paths

Severity: Minor

In function `update_path` in `cw-dex-router/src/contract.rs:231-249`, the contract admin is able to add swap paths to enable the liquidation of tokens that both do and do not share a direct pool. Currently, the contract validates that the first and last assets match the offer and ask assets. In the case that there are swap operations performed there may be a situation where intermediary assets do not match.

This would cause the failure of any execution of the function `basket_liquidate`.

We consider this a minor issue as the admin controls the addition of swap paths.

Recommendation

We recommend performing validation of every step in a `SwapOperationsList` prior to storage of a swap path.

Status: Resolved

5. Insufficient validation of vault configuration

Severity: Minor

When instantiating and updating the config of a vault, the function `check` is called in `apollo-vaults/packages/apollo-vault/src/state.rs87-110` which insufficiently validates the `performance_fee` to ensure that it is less than `Decimal::one()`.

Specifying a performance fee of greater than `Decimal::one()` would cause an overflow in `apollo-vaults/packages/apollo-vault/src/state.rs:94`.

Additionally, `reward_liquidation_target` is not enforced to be one of the assets in the pool as specified in lines `32-34`, which could potentially cause inconsistencies in the overall behavior of the vault.

Recommendation

We recommend validating that the `performance_fee` is less than `Decimal::one()` during instantiation and update.

In addition, we recommend querying the assets in the pool and validating that the submitted `reward_liquidation_target` is one of them.

Status: Resolved

6. Basket liquidation fails if no path is found for offer asset

Severity: Minor

In `cw-dex-router/src/contract.rs:251-305`, the `basket_liquidate` function swaps all offer assets into a single receive asset. The swap paths that are used to exchange the offer for the receive asset are defined by the contract admin.

In the case that one of the offer assets does not have a path set to the receive asset the contract will throw an error in `cw-dex-router/src/contract.rs:276`. This would prevent the execution of both the basket liquidation and the original calling function, `execute_compound` found in `apollo-vault/src/execute_compound.rs`, but also the primary function of the relevant vault.

We consider this only a minor issue as the swap paths are defined by the contract admin.

Recommendation

We recommend that in this scenario, instead of returning an error, `offer_assets` without swap paths should be appended to a list and emitted as an event to enable the continued execution of the vault.

Status: Resolved

7. Lack of Osmosis Vault parameter validation

Severity: Minor

The `osmosis-vault` contract from Apollo vaults' `instantiate` function does not validate the submitted `msg.pool_id` before storing it. This might cause two different vaults to coexist with the same ID but different base and vault tokens, potentially confusing users.

In addition, it is recommended to validate `msg.lockup_duration` to be within the expected range to avoid creating either a zero or an arbitrarily large lockup duration by mistake.

Recommendation

We recommend verifying that the `pool_id` is not in use. In addition, the lockup validation should be checked to be within an expected range of values.

Status: Resolved

8. Use of magic numbers throughout the codebase

Severity: Informational

Throughout the codebase, hard-coded number literals without context or a description are used. Using such "magic numbers" goes against best practices as they reduce code readability and maintenance as developers are unable to easily understand their use and may make inconsistent changes across the codebase.

Instances of magic numbers are listed below:

- `astroport-liquidity-helper/src/contract.rs:62`
- `astroport-liquidity-helper/src/contract.rs:95`
- `cw-dex/src/implementations/astroport/helpers:185-186`

Recommendation

We recommend defining magic numbers as constants with descriptive variable names and comments, where necessary.

Status: Acknowledged

The client has chosen to keep the magic numbers because they are based on the original Astroport implementation.

9. Additional funds sent to the contract are lost

Severity: Informational

In `apollo-vaults/packages/apollo-vault/src/execute_staking.rs:46`, a check is performed that ensures that in the transaction the desired native assets have been received.

This validation does not ensure that no other native tokens are sent though, and any additional native tokens are not returned to the user, so they will be stuck in the contract forever.

Recommendation

We recommend checking that the transaction contains only the expected native assets.

Status: Resolved

10. “Migrate only if newer” pattern not followed

Severity: Informational

The contracts within the scope of this audit can be migrated without validation that the new version is newer than the current version. This may lead to a migration being applied to (accidentally) downgrade a contract, which may have devastating consequences.

Recommendation

It is recommended to follow the migrate “only if newer” pattern defined in the CosmWasm documentation.

Status: Resolved

11. Unimplemented query entrypoint in liquidity helper causes panic

Severity: Informational

The `query` entrypoint in `osmosis-liquidity-helper:src/contract.rs:207` is currently unimplemented and will panic when it is queried.

Recommendation

We recommend implementing the query entrypoint or returning a descriptive error message.

Status: Resolved

12. Remove duplicate query functions

Severity: Informational

In both the Astroport Vault and the Osmosis Vault the `PreviewDeposit` and `ConvertToShares` queries call the same function. This is also true for the `PreviewRedeem` and `ConvertToAssets` queries.

Recommendation

We recommend removing this duplication and only providing one query per query function.

Status: Acknowledged

The client has chosen to keep the query functions unchanged because the queries are part of the vault standard. This will be a useful interface for functionality to be implemented in the future.

13. Redundant asset validation

Severity: Informational

The `astroport-vault` contract from Apollo vaults performs validation of `msg.base_token` in `contracts/astroport-vault/src/contract.rs:44`, assigning it to the `base_token` variable. However, later in line `54`, instead of using the result of the previous result `msg.base_token.check(deps.api)` is called again.

Recommendation

We recommend substituting `msg.base_token.check(deps.api)` for `base_token` in line `54`, as shown below:

```
// Validate that config.base_token is the same as the pool lp token
let lp_token_addr = match base_token {
```

Status: Resolved

14. Lack of clear function on admin two-step transfer mechanism

Severity: Informational

The `apollo-vault` package from Apollo vaults implements a two-step transfer mechanism for updating the `Admin` address, following best practices.

However, in order to remove a new admin address submitted by mistake, the current admin would have to call `execute_update_admin` again and overwrite the address. Although effective in practice, it will make more sense to have a function with the sole purpose of clearing this value.

Recommendation

We recommend adding a new entry point and function to the two-step transfer feature that allows the current admin to drop the value of `self.admin_transfer`.

Status: Resolved

15. Inconsistent usage of generic error

Severity: Informational

The Astroport pool implementation in `apollodao-cw-dex` returns a generic `"Either asset cannot be zero"` error if any of the deposited assets is zero in `src/implementations/astroport/pool.rs:102`, instead of the custom error `CwDexError::InvalidZeroAmount` as done in line `157`.

Although not a security issue, consistent error handling improves readability and maintainability.

Recommendation

We recommend returning the `CwDexError::InvalidZeroAmount` error instead.

Status: Resolved

16. Outdated dependencies

Severity: Informational

The contracts and libraries within the scope of this audit use outdated dependencies. Some cases are minor deviations from the latest version, however, there is an unmaintained dependency and one affected by a publicly known security vulnerability.

Unmaintained dependency:

- `dotenv`

Known vulnerabilities:

- CVE-2020-26235, `time 0.1.45` in use

This issue has been raised as informational as this vulnerability does not seem exploitable on the CosmWasm VM and the contract does not use the affected functions.

Further details on the outdated libraries can be found in Appendix A: Outdated dependencies.

Recommendation

We recommend updating the dependencies to the latest stable version of the libraries.

Status: Resolved

Appendix A: Outdated dependencies

to paste raw output from cargo audit and cargo outdated

`audit-apollodao-cw-vault-token`

Name	Project	Compat	Latest	Kind	Platform
cosmwasm-crypto->digest	0.10.5	0.10.6	0.10.6	Normal	---
cosmwasm-derive->syn	1.0.103	1.0.105	1.0.105	Normal	---
cosmwasm-schema	1.1.5	1.1.8	1.1.8	Normal	---
cosmwasm-schema->cosmwasm-schema-derive	1.1.5	1.1.8	1.1.8	Normal	---
cosmwasm-schema->serde	1.0.147	1.0.149	1.0.149	Normal	---
cosmwasm-schema->serde_json	1.0.87	1.0.89	1.0.89	Normal	---
cosmwasm-schema-derive->syn	1.0.103	1.0.105	1.0.105	Normal	---
cosmwasm-std	1.1.5	1.1.8	1.1.8	Normal	---
cosmwasm-std->cosmwasm-crypto	1.1.5	1.1.8	1.1.8	Normal	cfg(not(target_arch = "wasm32"))
cosmwasm-std->cosmwasm-derive	1.1.5	1.1.8	1.1.8	Normal	---
cosmwasm-std->serde	1.0.147	1.0.149	1.0.149	Normal	---
cosmwasm-std->uint	0.9.4	0.9.5	0.9.5	Normal	---
cpufeatures->libc	0.2.137	0.2.138	0.2.138	Normal	aarch64-apple-darwin
crypto-common->typenum	1.15.0	1.16.0	1.16.0	Normal	---
cw-storage-plus->cosmwasm-std	1.1.5	1.1.8	1.1.8	Normal	---
cw-storage-plus->serde	1.0.147	1.0.149	1.0.149	Normal	---
cw-utils	0.16.0	---	1.0.0	Normal	---
cw-utils->cosmwasm-schema	1.1.5	1.1.8	1.1.8	Normal	---
cw-utils->cosmwasm-std	1.1.5	1.1.8	1.1.8	Normal	---
cw-utils->serde	1.0.147	1.0.149	1.0.149	Normal	---
cw2->cosmwasm-schema	1.1.5	1.1.8	1.1.8	Normal	---
cw2->cosmwasm-std	1.1.5	1.1.8	1.1.8	Normal	---
cw2->serde	1.0.147	1.0.149	1.0.149	Normal	---
cw20	0.16.0	---	1.0.0	Normal	---
cw20->cosmwasm-schema	1.1.5	1.1.8	1.1.8	Normal	---
cw20->cosmwasm-std	1.1.5	1.1.8	1.1.8	Normal	---
cw20->serde	1.0.147	1.0.149	1.0.149	Normal	---
cw20-base	0.16.0	---	1.0.0	Normal	---
cw20-base->cosmwasm-schema	1.1.5	1.1.8	1.1.8	Normal	---
cw20-base->cosmwasm-std	1.1.5	1.1.8	1.1.8	Normal	---
cw20-base->cw2	0.16.0	---	1.0.0	Normal	---
cw20-base->cw20	0.16.0	---	1.0.0	Normal	---
cw20-base->serde	1.0.147	1.0.149	1.0.149	Normal	---
derivative->syn	1.0.103	1.0.105	1.0.105	Normal	---
ed25519-zebra->serde	1.0.147	1.0.149	1.0.149	Normal	---
elliptic-curve->digest	0.10.5	0.10.6	0.10.6	Normal	---
generic-array->typenum	1.15.0	1.16.0	1.16.0	Normal	---
getrandom->libc	0.2.137	0.2.138	0.2.138	Normal	cfg(unix)
hmac->digest	0.10.5	0.10.6	0.10.6	Normal	---
osmosis-std->cosmwasm-std	1.1.5	1.1.8	1.1.8	Normal	---
osmosis-std->prost	0.11.2	0.11.3	0.11.3	Normal	---
osmosis-std->serde	1.0.147	1.0.149	1.0.149	Normal	---
osmosis-std-derive->syn	1.0.103	1.0.105	1.0.105	Normal	---
prost->bytes	1.2.1	1.3.0	1.3.0	Normal	---
prost-derive->syn	1.0.103	1.0.105	1.0.105	Normal	---
prost-types->bytes	1.2.1	1.3.0	1.3.0	Normal	---
prost-types->prost	0.11.2	0.11.3	0.11.3	Normal	---
schemars->serde	1.0.147	1.0.149	1.0.149	Normal	---
schemars->serde_json	1.0.87	1.0.89	1.0.89	Normal	---

```
schemars_derive->syn                    1.0.103  1.0.105  1.0.105  Normal  ---
serde->serde_derive                     1.0.147  1.0.149  1.0.149  Normal  ---
serde-cw-value->serde                   1.0.147  1.0.149  1.0.149  Normal  ---
serde-json-wasm->serde                  1.0.147  1.0.149  1.0.149  Normal  ---
serde_derive->syn                       1.0.103  1.0.105  1.0.105  Normal  ---
serde_derive_internals->syn             1.0.103  1.0.105  1.0.105  Normal  ---
serde_json->serde                       1.0.147  1.0.149  1.0.149  Normal  ---
sha2->digest                            0.10.5   0.10.6   0.10.6   Normal  ---
signature->digest                       0.10.5   0.10.6   0.10.6   Normal  ---
thiserror-impl->syn                     1.0.103  1.0.105  1.0.105  Normal  ---
```

audit-apollodao-apollo-utils

```
Name                    Project  Compat   Latest   Kind    Platform
----                    -------  ------   ------   ----    --------
cosmwasm-schema->serde  1.0.148  1.0.149  1.0.149  Normal  ---
cosmwasm-std->serde     1.0.148  1.0.149  1.0.149  Normal  ---
crypto-common->typenum  1.15.0   1.16.0   1.16.0   Normal  ---
cw-asset->serde         1.0.148  1.0.149  1.0.149  Normal  ---
cw-storage-plus->serde  1.0.148  1.0.149  1.0.149  Normal  ---
cw-utils->serde         1.0.148  1.0.149  1.0.149  Normal  ---
cw2->serde              1.0.148  1.0.149  1.0.149  Normal  ---
cw20                    0.16.0   ---      1.0.0    Normal  ---
cw20->serde             1.0.148  1.0.149  1.0.149  Normal  ---
ed25519-zebra->serde    1.0.148  1.0.149  1.0.149  Normal  ---
generic-array->typenum  1.15.0   1.16.0   1.16.0   Normal  ---
schemars->serde         1.0.148  1.0.149  1.0.149  Normal  ---
serde->serde_derive     1.0.148  1.0.149  1.0.149  Normal  ---
serde-json-wasm->serde  1.0.148  1.0.149  1.0.149  Normal  ---
serde_json->serde       1.0.148  1.0.149  1.0.149  Normal  ---
```

audit-apollodao-apollo-vaults

```
Crate:     time
Version:   0.1.45
Title:     Potential segfault in the time crate
Date:      2020-11-18
ID:        RUSTSEC-2020-0071
URL:       https://rustsec.org/advisories/RUSTSEC-2020-0071
Solution:  Upgrade to >=0.2.23
Dependency tree:
time 0.1.45
└── chrono 0.4.23
    ├── osmosis-std 0.12.0
    ├── osmosis-std 0.12.0
    ├── osmosis-std 0.12.0
    ├── bollard-stubs 1.41.0
    │   ├── testcontainers 0.14.0
    │   │   └── cw-it 0.1.0
    │   │       └── osmosis-vault 0.1.0
    │   └── bollard 0.11.1
    │       └── testcontainers 0.14.0
    └── bollard 0.11.1

Crate:     dotenv
Version:   0.15.0
Warning:   unmaintained
Title:     dotenv is Unmaintained
Date:      2021-12-24
```

```
ID:          RUSTSEC-2021-0141
URL:         https://rustsec.org/advisories/RUSTSEC-2021-0141
Dependency tree:
dotenv 0.15.0
└── cw-it 0.1.0
    └── osmosis-vault 0.1.0

error: 1 vulnerability found!
warning: 1 allowed warning found
```

audit-apollodao-astroport-liquidity-helper

```
Crate:     time
Version:   0.1.45
Title:     Potential segfault in the time crate
Date:      2020-11-18
ID:        RUSTSEC-2020-0071
URL:       https://rustsec.org/advisories/RUSTSEC-2020-0071
Solution:  Upgrade to >=0.2.23
Dependency tree:
time 0.1.45
└── chrono 0.4.23
    ├── osmosis-std 0.12.0
    ├── osmosis-std 0.12.0
    ├── bollard-stubs 1.41.0
    │   ├── testcontainers 0.14.0
    │   │   └── cw-it 0.1.0
    │   │       └── astroport-liquidity-helper 0.1.0
    │   └── bollard 0.11.1
    │       └── testcontainers 0.14.0
    └── bollard 0.11.1

Crate:     dotenv
Version:   0.15.0
Warning:   unmaintained
Title:     dotenv is Unmaintained
Date:      2021-12-24
ID:        RUSTSEC-2021-0141
URL:       https://rustsec.org/advisories/RUSTSEC-2021-0141
Dependency tree:
dotenv 0.15.0
└── cw-it 0.1.0
    └── astroport-liquidity-helper 0.1.0

error: 1 vulnerability found!
warning: 1 allowed warning found
```

audit-apollodao-osmosis-liquidity-helper

```
Crate:     time
Version:   0.1.45
Title:     Potential segfault in the time crate
Date:      2020-11-18
ID:        RUSTSEC-2020-0071
URL:       https://rustsec.org/advisories/RUSTSEC-2020-0071
Solution:  Upgrade to >=0.2.23
Dependency tree:
time 0.1.45
└── chrono 0.4.23
```

```
    ├── osmosis-std 0.12.0
    │   ├── osmosis-testing 0.12.0
    │   │   ├── osmosis-liquidity-helper 0.1.0
    │   │   └── cw-it 0.1.0
    │   │       └── osmosis-liquidity-helper 0.1.0
    │   └── cw-dex 0.0.1
    │       └── osmosis-liquidity-helper 0.1.0
    ├── bollard-stubs 1.41.0
    │   ├── testcontainers 0.14.0
    │   │   └── cw-it 0.1.0
    │   └── bollard 0.11.1
    │       └── testcontainers 0.14.0
    └── bollard 0.11.1

Crate:     dotenv
Version:   0.15.0
Warning:   unmaintained
Title:     dotenv is Unmaintained
Date:      2021-12-24
ID:        RUSTSEC-2021-0141
URL:       https://rustsec.org/advisories/RUSTSEC-2021-0141
Dependency tree:
dotenv 0.15.0
└── cw-it 0.1.0
    └── osmosis-liquidity-helper 0.1.0

error: 1 vulnerability found!
warning: 1 allowed warning found
```

audit-apollodao-cw-dex

```
Name                                  Project                 Compat   Latest   Kind    Platform
----                                  -------                 ------   ------   ----    --------
ahash->getrandom                      0.2.8                   Removed  Removed  Normal
ahash->once_cell                      1.16.0                  Removed  Removed  Normal
cfg(not(all(target_arch = "arm", target_os = "none")))
ahash->version_check                  0.9.4                   Removed  Removed  Build   ---
block-buffer->generic-array           0.14.6                  Removed  Removed  Normal  ---
cosmwasm-crypto->digest               0.10.6                  Removed  Removed  Normal  ---
cosmwasm-crypto->ed25519-zebra        3.1.0                   Removed  Removed  Normal  ---
cosmwasm-crypto->k256                 0.11.6                  Removed  Removed  Normal  ---
cosmwasm-crypto->rand_core            0.6.4                   Removed  Removed  Normal  ---
cosmwasm-crypto->thiserror            1.0.37                  Removed  Removed  Normal  ---
cosmwasm-derive->syn                  1.0.104                 1.0.105  1.0.105  Normal  ---
cosmwasm-derive->syn                  1.0.104                 Removed  Removed  Normal  ---
cosmwasm-schema->cosmwasm-schema-derive 1.1.8                 Removed  ---      Normal  ---
cosmwasm-schema->schemars             0.8.11                  Removed  ---      Normal  ---
cosmwasm-schema->serde                1.0.148                 1.0.149  1.0.149  Normal  ---
cosmwasm-schema->serde_json           1.0.89                  Removed  ---      Normal  ---
cosmwasm-schema->thiserror            1.0.37                  Removed  ---      Normal  ---
cosmwasm-schema-derive->proc-macro2   1.0.47                  Removed  ---      Normal  ---
cosmwasm-schema-derive->quote         1.0.21                  Removed  ---      Normal  ---
cosmwasm-schema-derive->syn           1.0.104                 1.0.105  1.0.105  Normal  ---
cosmwasm-std->base64                  0.13.1                  Removed  Removed  Normal  ---
cosmwasm-std->cosmwasm-crypto         1.1.8                   Removed  Removed  Normal
cfg(not(target_arch = "wasm32"))
cosmwasm-std->cosmwasm-derive         1.1.8                   Removed  Removed  Normal  ---
cosmwasm-std->derivative              2.2.0                   Removed  Removed  Normal  ---
cosmwasm-std->forward_ref             1.0.0                   Removed  Removed  Normal  ---
cosmwasm-std->hex                     0.4.3                   Removed  Removed  Normal  ---
cosmwasm-std->schemars                0.8.11                  Removed  Removed  Normal  ---
cosmwasm-std->serde                   1.0.148                 1.0.149  1.0.149  Normal  ---
cosmwasm-std->serde                   1.0.148                 Removed  Removed  Normal  ---
cosmwasm-std->serde-json-wasm         0.4.1                   Removed  Removed  Normal  ---
cosmwasm-std->thiserror               1.0.37                  Removed  Removed  Normal  ---
```

```
cosmwasm-std->uint                    0.9.4                    0.9.5    0.9.5    Normal  ---
cosmwasm-std->uint                    0.9.4                    Removed  Removed  Normal  ---
cosmwasm-storage->serde               1.0.148                  1.0.149  1.0.149  Normal  ---
cpufeatures->libc                     0.2.137                  0.2.138  0.2.138  Normal
aarch64-apple-darwin
crypto-bigint->generic-array          0.14.6                   Removed  Removed  Normal  ---
crypto-bigint->rand_core              0.6.4                    Removed  Removed  Normal  ---
crypto-bigint->subtle                 2.4.1                    Removed  Removed  Normal  ---
crypto-bigint->zeroize                1.5.7                    Removed  Removed  Normal  ---
crypto-common->generic-array          0.14.6                   Removed  Removed  Normal  ---
crypto-common->typenum                1.15.0                   1.16.0   1.16.0   Normal  ---
curve25519-dalek->byteorder           1.4.3                    Removed  Removed  Normal  ---
curve25519-dalek->digest              0.9.0                    Removed  Removed  Normal  ---
curve25519-dalek->rand_core           0.5.1                    Removed  Removed  Normal  ---
curve25519-dalek->subtle              2.4.1                    Removed  Removed  Normal  ---
curve25519-dalek->zeroize             1.5.7                    Removed  Removed  Normal  ---
cw-asset->serde                       1.0.148                  1.0.149  1.0.149  Normal  ---
cw-controllers->serde                 1.0.148                  1.0.149  1.0.149  Normal  ---
cw-storage-plus                       0.16.0                   ---      1.0.1    Normal  ---
cw-storage-plus->cosmwasm-std         1.1.8                    Removed  ---      Normal  ---
cw-storage-plus->schemars             0.8.11                   Removed  ---      Normal  ---
cw-storage-plus->serde                1.0.148                  1.0.149  1.0.149  Normal  ---
cw-utils                              0.16.0                   0.11.1   1.0.0    Normal  ---
cw-utils->cosmwasm-schema             1.1.8                    Removed  ---      Normal  ---
cw-utils->cw2                         0.16.0                   Removed  ---      Normal  ---
cw-utils->semver                      1.0.14                   Removed  ---      Normal  ---
cw-utils->serde                       1.0.148                  1.0.149  1.0.149  Normal  ---
cw0->cosmwasm-std                     1.1.8                    Removed  Removed  Normal  ---
cw0->schemars                         0.8.11                   Removed  Removed  Normal  ---
cw0->serde                            1.0.148                  1.0.149  1.0.149  Normal  ---
cw0->serde                            1.0.148                  Removed  Removed  Normal  ---
cw0->thiserror                        1.0.37                   Removed  Removed  Normal  ---
cw2->cosmwasm-schema                  1.1.8                    Removed  ---      Normal  ---
cw2->cosmwasm-std                     1.1.8                    Removed  ---      Normal  ---
cw2->cw-storage-plus                  0.16.0                   Removed  ---      Normal  ---
cw2->schemars                         0.8.11                   Removed  ---      Normal  ---
cw2->serde                            1.0.148                  1.0.149  1.0.149  Normal  ---
cw20                                  0.10.3                   0.16.0   1.0.0    Normal  ---
cw20->cw0                             0.10.3                   Removed  Removed  Normal  ---
cw20->serde                           1.0.148                  1.0.149  1.0.149  Normal  ---
cw20-base->serde                      1.0.148                  1.0.149  1.0.149  Normal  ---
der->const-oid                        0.9.1                    Removed  Removed  Normal  ---
der->zeroize                          1.5.7                    Removed  Removed  Normal  ---
derivative->proc-macro2               1.0.47                   Removed  Removed  Normal  ---
derivative->quote                     1.0.21                   Removed  Removed  Normal  ---
derivative->syn                       1.0.104                  1.0.105  1.0.105  Normal  ---
derivative->syn                       1.0.104                  Removed  1.0.105  Normal  ---
derivative->syn                       1.0.104                  Removed  Removed  Normal  ---
digest->block-buffer                  0.10.3                   Removed  Removed  Normal
digest->crypto-common                 0.1.6                    Removed  Removed  Normal  ---
digest->generic-array                 0.14.6                   Removed  Removed  Normal  ---
digest->subtle                        2.4.1                    Removed  Removed  Normal  ---
ecdsa->der                            0.6.0                    Removed  Removed  Normal  ---
ecdsa->elliptic-curve                 0.12.3                   Removed  Removed  Normal  ---
ecdsa->rfc6979                        0.3.1                    Removed  Removed  Normal  ---
ecdsa->signature                      1.6.4                    Removed  Removed  Normal  ---
ed25519-zebra->curve25519-dalek       3.2.0                    Removed  Removed  Normal  ---
ed25519-zebra->hashbrown              0.12.3                   Removed  Removed  Normal  ---
ed25519-zebra->hex                    0.4.3                    Removed  Removed  Normal  ---
ed25519-zebra->rand_core              0.6.4                    Removed  Removed  Normal  ---
ed25519-zebra->serde                  1.0.148                  1.0.149  1.0.149  Normal
ed25519-zebra->sha2                   0.9.9                    Removed  Removed  Normal  ---
ed25519-zebra->zeroize                1.5.7                    Removed  Removed  Normal  ---
elliptic-curve->base16ct              0.1.1                    Removed  Removed  Normal  ---
elliptic-curve->crypto-bigint         0.4.9                    Removed  Removed  Normal  ---
elliptic-curve->der                   0.6.0                    Removed  Removed  Normal  ---
elliptic-curve->digest                0.10.6                   Removed  Removed  Normal  ---
elliptic-curve->ff                    0.12.1                   Removed  Removed  Normal  ---
elliptic-curve->generic-array         0.14.6                   Removed  Removed  Normal  ---
elliptic-curve->group                 0.12.1                   Removed  Removed  Normal  ---
```

```
elliptic-curve->pkcs8                    0.9.0                          Removed  Removed  Normal  ---
elliptic-curve->rand_core                0.6.4                          Removed  Removed  Normal  ---
elliptic-curve->sec1                     0.3.0                          Removed  Removed  Normal  ---
elliptic-curve->subtle                   2.4.1                          Removed  Removed  Normal
elliptic-curve->zeroize                  1.5.7                          Removed  Removed  Normal
ff->rand_core                            0.6.4                          Removed  Removed  Normal  ---
ff->subtle                               2.4.1                          Removed  Removed  Normal  ---
generic-array->typenum                   1.15.0                         1.16.0   1.16.0   Normal  ---
generic-array->version_check             0.9.4                          Removed  Removed  Build   ---

getrandom->cfg-if                        1.0.0                          Removed  Removed  Normal  ---
getrandom->libc                          0.2.137                        0.2.138  0.2.138  Normal  cfg(unix)
getrandom->wasi                          0.11.0+wasi-snapshot-preview1  Removed  Removed  Normal  cfg(target_os =
"wasi")

group->ff                                0.12.1                         Removed  Removed  Normal  ---
group->rand_core                         0.6.4                          Removed  Removed  Normal  ---
group->subtle                            2.4.1                          Removed  Removed  Normal  ---
hashbrown->ahash                         0.7.6                          Removed  Removed  Normal  ---
hmac->digest                             0.10.6                         Removed  Removed  Normal  ---
k256->cfg-if                             1.0.0                          Removed  Removed  Normal  ---
k256->ecdsa                              0.14.8                         Removed  Removed  Normal  ---
k256->elliptic-curve                     0.12.3                         Removed  Removed  Normal  ---
k256->sha2                               0.10.6                         Removed  Removed  Normal  ---
osmosis-std->prost                       0.11.2                         0.11.3   0.11.3   Normal  ---
osmosis-std->serde                       1.0.148                        1.0.149  1.0.149  Normal  ---
osmosis-std-derive->syn                  1.0.104                        1.0.105  1.0.105  Normal  ---
pkcs8->der                               0.6.0                          Removed  Removed  Normal  ---
pkcs8->spki                              0.6.0                          Removed  Removed  Normal  ---
proc-macro2->unicode-ident               1.0.5                          Removed  Removed  Normal  ---
prost-derive->syn                        1.0.104                        1.0.105  1.0.105  Normal  ---
prost-types->prost                       0.11.2                         0.11.3   0.11.3   Normal  ---
quote->proc-macro2                       1.0.47                         Removed  Removed  Normal  ---
rand_core->getrandom                     0.2.8                          Removed  Removed  Normal  ---
rfc6979->crypto-bigint                   0.4.9                          Removed  Removed  Normal  ---
rfc6979->hmac                            0.12.1                         Removed  Removed  Normal  ---
rfc6979->zeroize                         1.5.7                          Removed  Removed  Normal  ---
schemars->dyn-clone                      1.0.9                          Removed  Removed  Normal  ---
schemars->schemars_derive                0.8.11                         Removed  Removed  Normal  ---
schemars->serde                          1.0.148                        1.0.149  1.0.149  Normal  ---
schemars->serde_json                     1.0.89                         Removed  Removed  Normal  ---
schemars_derive->proc-macro2             1.0.47                         Removed  Removed  Normal  ---
schemars_derive->quote                   1.0.21                         Removed  Removed  Normal  ---
schemars_derive->serde_derive_internals  0.26.0                         Removed  Removed  Normal  ---
schemars_derive->syn                     1.0.104                        1.0.105  1.0.105  Normal  ---
sec1->base16ct                           0.1.1                          Removed  Removed  Normal  ---
sec1->der                                0.6.0                          Removed  Removed  Normal  ---
sec1->generic-array                      0.14.6                         Removed  Removed  Normal  ---
sec1->pkcs8                              0.9.0                          Removed  Removed  Normal  ---
sec1->subtle                             2.4.1                          Removed  Removed  Normal  ---
sec1->zeroize                            1.5.7                          Removed  Removed  Normal  ---
serde->serde_derive                      1.0.148                        1.0.149  1.0.149  Normal  ---
serde-cw-value->serde                    1.0.148                        1.0.149  1.0.149  Normal  ---
serde-json-wasm->serde                   1.0.148                        Removed  1.0.149  Normal  ---
serde_derive->proc-macro2                1.0.47                         Removed  Removed  Normal  ---
serde_derive->quote                      1.0.21                         Removed  Removed  Normal  ---
serde_derive->syn                        1.0.104                        1.0.105  1.0.105  Normal  ---
serde_derive_internals->proc-macro2      1.0.47                         Removed  Removed  Normal  ---
serde_derive_internals->quote            1.0.21                         Removed  Removed  Normal  ---
serde_derive_internals->syn              1.0.104                        1.0.105  1.0.105  Normal  ---
serde_json->itoa                         1.0.4                          Removed  Removed  Normal  ---
serde_json->ryu                          1.0.11                         Removed  Removed  Normal  ---
serde_json->serde                        1.0.148                        1.0.149  1.0.149  Normal  ---
sha2->block-buffer                       0.9.0                          Removed  Removed  Normal  ---
sha2->cfg-if                             1.0.0                          Removed  Removed  Normal  ---
sha2->cpufeatures                        0.2.5                          Removed  Removed  Normal
cfg(any(target_arch = "aarch64", target_arch = "x86_64", target_arch = "x86"))
sha2->digest                             0.10.6                         Removed  Removed  Normal  ---
sha2->digest                             0.9.0                          Removed  Removed  Normal  ---
sha2->opaque-debug                       0.3.0                          Removed  Removed  Normal  ---
```

```
signature->digest                         0.10.6                        Removed  Removed  Normal  ---
signature->rand_core                      0.6.4                         Removed  Removed  Normal  ---
spki->base64ct                            1.5.3                         Removed  Removed  Normal  ---
spki->der                                 0.6.0                         Removed  Removed  Normal  ---
stake-cw20->serde                         1.0.148                       1.0.149  1.0.149  Normal  ---
syn->proc-macro2                          1.0.47                        Removed  Removed  Normal  ---
syn->quote                                1.0.21                        Removed  Removed  Normal  ---
syn->unicode-ident                        1.0.5                         Removed  Removed  Normal  ---
thiserror->thiserror-impl                 1.0.37                        Removed  Removed  Normal  ---
thiserror-impl->proc-macro2               1.0.47                        Removed  Removed  Normal  ---
thiserror-impl->quote                     1.0.21                        Removed  Removed  Normal  ---
thiserror-impl->syn                       1.0.104                       1.0.105  1.0.105  Normal  ---
uint                                      0.9.4                         0.9.5    0.9.5    Normal  ---
uint->byteorder                           1.4.3                         Removed  Removed  Normal  ---
uint->crunchy                             0.2.2                         Removed  Removed  Normal  ---
uint->hex                                 0.4.3                         Removed  Removed  Normal  ---
uint->static_assertions                   1.1.0                         Removed  Removed  Normal  ---
wasmswap->serde                           1.0.148                       1.0.149  1.0.149  Normal  ---
```

audit-apollodao-cw-dex-router

```
Crate:     time
Version:   0.1.45
Title:     Potential segfault in the time crate
Date:      2020-11-18
ID:        RUSTSEC-2020-0071
URL:       https://rustsec.org/advisories/RUSTSEC-2020-0071
Solution:  Upgrade to >=0.2.23
Dependency tree:
time 0.1.45
└── chrono 0.4.23
    ├── osmosis-std 0.12.0
    │   ├── osmosis-testing 0.12.0
    │   │   ├── cw-it 0.1.0
    │   │   │   └── cw-dex-router 0.1.0
    │   │   └── cw-dex-router 0.1.0
    │   └── cw-dex 0.0.1
    │       └── cw-dex-router 0.1.0
    ├── bollard-stubs 1.41.0
    │   ├── testcontainers 0.14.0
    │   │   ├── cw-it 0.1.0
    │   │   └── cw-dex-router 0.1.0
    │   └── bollard 0.11.1
    │       └── testcontainers 0.14.0
    └── bollard 0.11.1

Crate:     dotenv
Version:   0.15.0
Warning:   unmaintained
Title:     dotenv is Unmaintained
Date:      2021-12-24
ID:        RUSTSEC-2021-0141
URL:       https://rustsec.org/advisories/RUSTSEC-2021-0141
Dependency tree:
dotenv 0.15.0
└── cw-it 0.1.0
    └── cw-dex-router 0.1.0

error: 1 vulnerability found!
warning: 1 allowed warning found
```