Quantstamp

API3 - Contracts

Executive Summary

This audit report was prepared by Quantstamp, the leader in blockchain security.

Type	Oracle
Timeline	2024-09-30 through 2024-10-14
Language	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Contract Docs
Source Code	• api3dao/contracts-qs #dcf18f4
Auditors	• Roman Rohleder Senior Auditing Engineer • Cameron Biniamow Auditing Engineer • Darren Jensen Auditing Engineer

Documentation quality	High
Test quality	High
Total Findings	3 Acknowledged: 1 Mitigated: 2
High severity findings	0
Medium severity findings	0
Low severity findings	1 Mitigated: 1
Undetermined severity findings	0
Informational findings	2 Acknowledged: 1 Mitigated: 1

Summary of Findings

API3 is a multi-chain oracle system for serving, updating, and monetizing decentralized API data feeds with features like OEV (Oracle Extractable Value) support and a subscription marketplace. This audit revolved around the newest version of the API3 contracts where the OEV-related logic from the `Api3ServerV1` contract is replicated and refactored in the `Api3ServerV1OevExtension` contract. The audit team reviewed the entire on-chain API3 system and verified that the contracts operate as expected.

The audit team determined that the codebase is high-quality, with thorough documentation and a robust test suite. During the review, the audit team identified one low-severity issue related to seekers avoiding fee payment. Additionally, this report lists two informational severity issues and ten auditor suggestions for adhering to best practices.

Update: The API3 team has fixed, mitigated, or acknowledged all issues listed in this report at commit hash `d7adea1c81755d57676ebdb12c9888f6617b3d38`. Due to many contracts already being deployed, the API3 team opted to acknowledge most of the issues in this report rather than redeploy the contracts with fixes. During the fix review, the API3 team also altered the functionality so that bidders could pay the bid fee in the `Api3ServerV1OevExtension` contract through a callback.

ID	DESCRIPTION	SEVERITY	STATUS
API3-1	**Seeker Can Avoid Paying Protocol or Collateral Fees if the Award Transaction Reverts**	Low	Mitigated
API3-2	`AirseekerRegistry` **Functions Uncallable**	Informational	Acknowledged
API3-3	**Index of Active Data Feeds Is Subject to Change**	Informational	Mitigated

Assessment Breakdown

Quantstamp's objective was to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices.

> **Disclaimer**
>
> Only features that are contained within the repositories at the commit hashes specified on the front page of the report are within the scope of the audit and fix review. All features added in future revisions of the code are excluded from consideration in this report.

Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Integer overflow / underflow
- Number rounding errors
- Reentrancy and cross-function vulnerabilities
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting

Methodology

1. Code review that includes the following
    1. Review of the specifications, sources, and instructions provided to Quantstamp to make sure we understand the size, scope, and functionality of the smart contract.
    2. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
    3. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Quantstamp describe.
2. Testing and automated analysis that includes the following:
    1. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
    2. Symbolic execution, which is analyzing a program to determine what inputs cause each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, and actionable recommendations to help you take steps to secure your smart contracts.

Scope

Files Included

- `contracts/access/GnosisSafeWithoutProxy.sol`
- `contracts/access/AccessControlRegistry.sol`
- `contracts/access/AccessControlRegistryAdminnedWithManager.sol`
- `contracts/access/RoleDeriver.sol`
- `contracts/access/HashRegistry.sol`
- `contracts/access/OwnableCallForwarder.sol`
- `contracts/access/AccessControlRegistryAdminned.sol`
- `contracts/access/interfaces/IOwnable.sol`
- `contracts/access/interfaces/IOwnableCallForwarder.sol`
- `contracts/access/interfaces/IAccessControlRegistry.sol`
- `contracts/access/interfaces/IHashRegistry.sol`
- `contracts/access/interfaces/IAccessControlRegistryAdminned.sol`
- `contracts/access/interfaces/IAccessControlRegistryAdminnedWithManager.sol`
- `contracts/utils/SelfMulticall.sol`
- `contracts/utils/ExtendedSelfMulticall.sol`
- `contracts/utils/interfaces/IExtendedSelfMulticall.sol`
- `contracts/utils/interfaces/ISelfMulticall.sol`
- `contracts/api3-server-v1/aggregation/Median.sol`
- `contracts/api3-server-v1/aggregation/QuickSelect.sol`
- `contracts/api3-server-v1/aggregation/Sort.sol`
- `contracts/api3-server-v1/Api3MarketV2.sol`
- `contracts/api3-server-v1/BeaconUpdatesWithSignedData.sol`
- `contracts/api3-server-v1/DapiServer.sol`
- `contracts/api3-server-v1/AirseekerRegistry.sol`
- `contracts/api3-server-v1/OevDataFeedServer.sol`
- `contracts/api3-server-v1/Api3ServerV1OevExtension.sol`
- `contracts/api3-server-v1/OevDapiServer.sol`
- `contracts/api3-server-v1/OevAuctionHouse.sol`
- `contracts/api3-server-v1/Api3ServerV1.sol`

- `contracts/api3-server-v1/DataFeedServer.sol`
- `contracts/api3-server-v1/proxies/Api3ReaderProxyV1.sol`
- `contracts/api3-server-v1/proxies/Api3ReaderProxyV1Factory.sol`
- `contracts/api3-server-v1/proxies/interfaces/IApi3ReaderProxyV1Factory.sol`
- `contracts/api3-server-v1/proxies/interfaces/IProxy.sol`
- `contracts/api3-server-v1/proxies/interfaces/IOevProxy.sol`
- `contracts/api3-server-v1/proxies/interfaces/IApi3ReaderProxyV1.sol`
- `contracts/api3-server-v1/interfaces/IOevDataFeedServer.sol`
- `contracts/api3-server-v1/interfaces/IApi3MarketV2.sol`
- `contracts/api3-server-v1/interfaces/IApi3ServerV1.sol`
- `contracts/api3-server-v1/interfaces/IOevAuctionHouse.sol`
- `contracts/api3-server-v1/interfaces/IDapiServer.sol`
- `contracts/api3-server-v1/interfaces/IBeaconUpdatesWithSignedData.sol`
- `contracts/api3-server-v1/interfaces/IAirseekerRegistry.sol`
- `contracts/api3-server-v1/interfaces/IOevDapiServer.sol`
- `contracts/api3-server-v1/interfaces/IApi3ServerV1OevExtension.sol`
- `contracts/api3-server-v1/interfaces/IDataFeedServer.sol`
- `contracts/interfaces/IApi3ReaderProxy.sol`

Operational Considerations

1. The `Api3ServerV1OevExtension` contract is used to collect bid amounts from searchers who execute an OEV opportunity. However, there is no direct payment to the beneficiary of the specific `dappId` the bid was intended for. Instead, the contract provides a `withdraw()` function, which needs to be called by a trusted `withdrawer` account. Therefore, this function should be called such that the `recipient` and `amount` are set correctly by the trusted `withdrawer` account to pay the beneficiary their share of the OEV bid.
2. The contract `Api3ReaderProxyV1.sol` is upgradable.
3. The OEV auction house heavily relies on off-chain computations and the correct and fair behavior of the auctioneer role.

Key Actors And Their Capabilities

- `AccessControlRegistry.sol`
  - This contract is deployed on each chain as a centralized access control contract. Other contracts in the system will refer to the `AccessControlRegistry` to validate a user's privileged roles. By design, the `AccessControlRegistry` contract enables any address to be a unique admin role where they can grant or revoke a set of derived privileged roles to any address.
- `AirseekerRegistry.sol`
  - `owner`
    - *Note: The `Api3MarketV2` contract is the owner of the `AirseekerRegistry` contract.*
    - Cannot transfer or renounce their ownership.
    - Can activate or deactivate a data feed by its ID.
    - Can activate or deactivate a dAPI by its name.
    - Can update a data feed's update parameters.
    - Can update an airnode's signed API URL.
- `Api3MarketV2.sol`
  - `owner`
    - Cannot transfer or renounce their ownership.
    - Can set the `AirseekerRegistry` contract address. Note that the `AirseekerRegistry` contract address can only be set once.
    - Can call `cancelSubscriptions()` to cancel any active subscription.
- `OevAuctionHouse.sol`
  - `manager`
    - Can call `setCollateralInBasisPoints()` to arbitrarily change the collateral basis points relative to a bid. **May be 0% or exceed 100%**.
    - Can call `setProtocolFeeInBasisPoints()` to arbitrarily change the protocol fee basis points relative to a bid. **May be 0% or exceed 100%**.
    - Can call `setCollateralRateProxy()` to change the collateral rate proxy address.
    - Can call `setChainNativeCurrencyRateProxy()` to change the native currency rate proxy address.
    - Can call `withdrawAccumulatedSlashedCollateral()` to retrieve slashed collateral from bidders.
    - Can call `withdrawAccumulatedProtocolFees()` to retrieve protocol fees.
  - `proxySetterRole`
    - Can call `setCollateralRateProxy()` to change the collateral rate proxy address.
    - Can call `setChainNativeCurrencyRateProxy()` to change the native currency rate proxy address.
  - `withdrawerRole`
    - Can call `withdrawAccumulatedSlashedCollateral()` to retrieve slashed collateral from bidders.
    - Can call `withdrawAccumulatedProtocolFees()` to retrieve protocol fees.
  - `auctioneerRole`
    - Can call `awardBid()` to award a bid to a bidder.
    - Can call `confirmFulfillment()` to confirm an awarded bidder processed their OEV update, which releases the bidder's collateral and deducts the protocol fee.

        - Can call `contradictFulfillment()` to contradict an awarded bid, which slashes the bidder's collateral.
- `Api3ServerV1OevExtension.sol`
    - `manager`
        - Can call `withdraw()` to withdraw and transfer OEV bids to dApp beneficiaries.
    - `withdrawerRole`
        - Can call `withdraw()` to withdraw and transfer OEV bids to dApp beneficiaries.
    - `lastPaidBid.updater`
        - Can call `updateDappOevDataFeed()` to process an OEV data feed update.
- `HashRegistry.sol`
    - `owner`
        - Can renounce their ownership.
        - Can transfer their ownership.
        - Can call `setSigners()` to set or update the signers for a given hash type.
        - Can call `setHash()` to set or update the hash for a hash type.
- `OwnableCallForwarder.sol`
    - `owner`
        - Can renounce their ownership.
        - Can transfer their ownership.
        - Can call `forwardCall()` to execute an arbitrary external call.
- `Api3ReaderProxyV1Factory.sol`
    - `owner`
        - Will be owner of all deployed `Api3ReaderProxyV1.sol` contracts through `deployApi3ReaderProxyV1()`.
        - Can renounce their ownership.
        - Can transfer their ownership.
- `Api3ReaderProxyV1.sol`
    - `owner`
        - Can authorize upgrades.
        - Can renounce their ownership.
        - Can transfer their ownership.

Findings

API3-1
Seeker Can Avoid Paying Protocol or Collateral Fees if the Award Transaction Reverts

Low Mitigated

Update

The client mitigated the issue in commit `f65c52ffb2664bcd6fc3cf8afd1f700ec56881fd` and provided the following explanation:

```
If an auctioneer is sending its transactions through a public mempool, a searcher can use their award
before the auctioneer transaction with the respective awardBid() call is confirmed. If this call
succeeds later, the searcher will still have to report having paid the bid amount to avoid being
slashed (which satisfies our requirements). On the other hand, if this call reverts later, the searcher
will not be slashed for their bid, which indeed corresponds to being able to perform OEV updates
without paying the respective bid amount.
  The solution to this is for the auctioneer to only send award transactions that are guaranteed
(within reasonable limits) to be confirmed. The documentation emphasizes the importance of the
auctioneer checking the bid expiration and the bidder balance, as these change outside the control of
the auctioneer. Compared to these, in the current auction design, there is a deterministic way to
choose a suitable awardExpirationTimestamp value.
  We extended the docs to explain how auctioneers should choose awardExpirationTimestamp.
```

File(s) affected: `OevAuctionHouse.sol`

Description: If the Auctioneer calling the `awardBid()` function sets the `awardExpirationTimestamp` such that the award transaction reverts while the specific OEV opportunity is still valid then the Seeker can execute the `awardDetails` without paying any protocol or collateral fees. This is because the Seeker may monitor the mempool for such transactions and execute them on-chain before the award transaction is finalized.

Recommendation: Ensure the Auctioneer calculates the `awardExpirationTimestamp` according to the `bidDetails` to avoid the award transaction from reverting too early.

API3-2 `AirseekerRegistry` Functions Uncallable

Informational Acknowledged

Update

The client acknowledged the issue and provided the following explanation:

> `Instead of having three versions of AirseekerRegistry (one that works with dAPI names, one that works with data feed IDs, and one that works with both), we only implemented one that works with both dAPI names and data feed IDs for it to be used for all three cases. This reduces clutter in return for potentially deploying redundant contract functionality (which applies in the case of Api3MarketV2), which we will stick by.`

File(s) affected: `AirseekerRegistry.sol`, `Api3MarketV2.sol`

Description: The `AirseekerRegistry.sol` contract may have its `owner` set only during the `constructor()` call since `transferOwnership()` has been disabled. For the `Api3MarketV2.sol` owner to be able to call `setAirseekerRegistry()`, the corresponding owner of the air seeker contract must be the market contract. This means that all `onlyOwner` modifier protected functions within `AirseekerRegistry.sol` should be exposed/callable by the market contract or otherwise can not be used. In particular, the following functions remain uncallable from the market contract:

1. `setDataFeedIdToBeActivated()`.
2. `setDataFeedIdToBeDeactivated()`.
3. `setDataFeedIdUpdateParameters()`.

Recommendation: We recommend exposing these functions to the market contract or to remove them.

API3-3 Index of Active Data Feeds Is Subject to Change

Informational · Mitigated

Update

The client mitigated the issue in commit `e4020a38ae676a881db53e22c46028967705cf8d` and provided the following explanation:

> `Added documentation about the fact.`

File(s) affected: `AirseekerRegistry.sol`

Description: In the function `AirseekerRegistry.activeDataFeed()`, the caller is expected to provide the `index` of an active data feed to retrieve the relevant information. However, as data feeds are activated and deactivated, the index of any data feed could change. Therefore, it is not possible for the caller to know if the `index` correctly corresponds to the desired data feed before `activeDataFeed()` is executed.

Recommendation: Clearly document that callers of `activeDataFeed()` must validate that the returned `dataFeedId` is correct.

Auditor Suggestions

S1 Critical Role Transfer Not Following Two-Step Pattern

Acknowledged

Update

The client acknowledged the suggestion and provided the following explanation:

> `We do not prefer Ownable2Step for the time being due to the friction it would introduce to our operations.`

File(s) affected: `OwnableCallForwarder.sol`, `Api3ReaderProxyV1Factory.sol`, `Api3ReaderProxyV1.sol`

Description: The owner of the contracts can call `transferOwnership()` to transfer the ownership to a new address. If an uncontrollable address is accidentally provided as the new owner address then the contract will no longer have an active owner, and functions with the `onlyOwner` modifier can no longer be executed.

Recommendation: Consider using OpenZeppelin's `Ownable2Step` contract to adopt a two-step ownership pattern in which the new owner must accept their position before the transfer is complete.

S2 Multiple Implementations of `deriveBeacon*Id()`

Acknowledged

Update

The client acknowledged the suggestion and provided the following explanation:

```
We will not address this because some of the contracts mentioned are deployed in production and are not intended to be replaced at this moment.
```

File(s) affected: `Api3MarketV2.sol`, `AirseekerRegistry.sol`, `DataFeedServer.sol`

Description: Functions `deriveBeaconId()` and `deriveBeaconSetId()` are defined in multiple contracts, leading to redundancy and increased maintainability.

Recommendation: We recommend outlining these functions i.e. into a shared `Utils.sol` contract to improve maintainability.

S3 Ownership Can Be Renounced

Acknowledged

Update

The client acknowledged the suggestion and provided the following explanation:

```
The ownership of the listed contracts are intended to be renounceable.
```

File(s) affected: `OwnableCallForwarder.sol`, `Api3ReaderProxyV1Factory.sol`, `Api3ReaderProxyV1.sol`

Description: If the owner renounces their ownership, all ownable contracts will be left without an owner. Consequently, any function guarded by the `onlyOwner` modifier will no longer be able to be executed.

Recommendation: Confirm that this is the intended behavior. If not, override and disable the `renounceOwnership()` function in the affected contracts. For extra security, consider using a two-step process when transferring the ownership of the contract (e.g. `Ownable2Step` from OpenZeppelin).

S4 Users Can Register Data Feeds Using a Zero Template ID

Acknowledged

Update

The client acknowledged the suggestion and provided the following explanation:

```
Template IDs being a hash value is considered to be convention and thus is not enforced on-chain.
Therefore, we do not necessarily consider a zero template ID to be invalid.
```

File(s) affected: `AirseekerRegistry.sol`

Description: The `AirseekerRegistry` contract allows any user to call the `registerDataFeed()` function to register a new Data Feed. However, there is no validation that the `templateId` for the new Data Feed is not zero, which can result in registering an unusable Data Feed.

Recommendation: Include a validation that `templateId` is non-zero when registering a new Data Feed.

S5 Set `HashRegistry` Signature Delegation Hash Type as a Constant

Fixed

Update

The client fixed the suggestion in commit `753245f8fd8c566f679328cea3665f8d554fa233` by creating the constant `HASHREGISTRY_SIGNATURE_DELEGATION_HASH_TYPE`.

File(s) affected: `HashRegistry.sol`

Description: The function `HashRegistry.signatureDelegationHashType()` hashes the same string each time it is called, resulting in redundant and excessive gas costs over the lifetime of the contract.

Recommendation: Consider creating a constant `SIGNATURE_DELEGATION_HASH_TYPE` that is set to the hash of `"HashRegistry signature delegation"` during contract construction.

S6 Cache Storage Variable

Acknowledged

Update

The client acknowledged the suggestion and provided the following explanation:

```
We will not address this because OevAuctionHouse is deployed in production and is not intended to be replaced at this moment.
```

File(s) affected: `OevAuctionHouse.sol`

Description: In the function `OevAuctionHouse.getCurrentCollateralAndProtocolFeeAmounts()`, the storage variables `collateralInBasisPoints` and `protocolFeeInBasisPoints` are loaded twice during the execution of the function resulting in excessive gas costs.

Recommendation: Cache the storage variables to reduce costly storage loads.

S7 Documentation Errors

Mitigated

Update

The client mitigated the suggestion in commit `09ab0cf28140d6d5c32cf346f327b6737cd00060` and provided the following explanation:

```
1. Fixed.
2. Acknowledged. The DapiProxy.sol that is referred to is an actual contract belonging to the previous
   iteration. We will not address this at this moment to not change the metadata hash of the already
   deployed OevAuctionHouse.
```

File(s) affected: `oevauctionhouse.md`, `IProxy.sol`

Description:

1. In `api3-server-v1/oevauctionhouse.md` under the **Off-chain protocol specs** section, it is stated that "*`updateDappOevDataFeedWithAllowedSignedData()` function is being called to update the OEV feed*". However, the function being called should be `updateDappOevDataFeed()`.
2. In `api3-server-v1/proxies/interfaces/IProxy.sol`, the NatSpec `@dev` comment refers to a `DapiProxy.sol` contract, which does not exist.

Recommendation: Consider fixing the mentioned documentation errors.

S8 Code Improvements

Mitigated

Update

The client mitigated the suggestion in commit `d7adea1c81755d57676ebdb12c9888f6617b3d38` and provided the following explanation:

```
1. Fixed.
2. Acknowledged. It is assumed that off-chain services will have indexed the respective PlacedBid
   event, from which the locked amount can be derived.
```

File(s) affected: `Api3ServerV1OevExtension.sol`, `OevAuctionHouse.sol`

Description:

1. At `api3-server-v1/Api3ServerV1OevExtension.sol#L415`, change the second parameter to use `baseDataFeedId` in `abi.encodePacked` since `baseDataFeedId` is already derived on `L412`.
2. At `api3-server-v1/OevAuctionHouse.sol#L649`, the `AwardedBid` event is emitted when the Auctioneer calls the `awardBid()` function. However, while it emits the `bidderBalance`, it would also be useful for off-chain services if the `lockedAmount` was included in the `AwardedBid` event parameters.

Recommendation: Consider implementing the mentioned code improvements.

S9 Set Parent Contracts as `abstract`

Acknowledged

Update

The client acknowledged the suggestion and provided the following explanation:

```
The abstract keyword also signals to the compiler to not complain about unimplemented interface
functions, which is why we do not prefer to use it to label contracts that are intended to be
inherited.
```

Description: The following contracts are not intended to be deployed as-is; instead, they are designed to be inherited by child contracts:

1. `RoleDeriver.sol`
2. `HashRegistry.sol`
3. `AccessControlRegistryAdminned.sol`
4. `AccessControlRegistryAdminnedWithManager.sol`
5. `SelfMulticall.sol`
6. `ExtendedSelfMulticall.sol`
7. `QuickSelect.sol`
8. `Sort.sol`
9. `Median.sol`
10. `DataFeedServer.sol`
11. `BeaconUpdatesWithSignedData.sol`
12. `OevDataFeedServer.sol`
13. `DapiServer.sol`
14. `OevDapiServer.sol`

Recommendation: Set the mentioned contracts as `abstract` for improved readability.

S10 Unlocked Pragma

Acknowledged

Update

The client acknowledged the suggestion and provided the following explanation:

> `We prefer to unlock the Solidity version for contracts that are expected to be inherited by contracts outside of this codebase.`

File(s) affected: `AccessControlRegistryAdminnedWithManager.sol`, `RoleDeriver.sol`, `AccessControlRegistryAdminned.sol`, `SelfMulticall.sol`, `ExtendedSelfMulticall.sol`, `Median.sol`, `QuickSelect.sol`, `Sort.sol`

Related Issue(s): SWC-103

Description: Every Solidity file specifies in the header a version number of the format `pragma solidity (^)0.8.*`. The caret (`^`) before the version number implies an unlocked pragma, meaning that the compiler will use the specified version *and above*, hence the term "unlocked".

Recommendation: For consistency and to prevent unexpected behavior in the future, we recommend to remove the caret to lock the file onto a specific Solidity version.

Definitions

- **High severity** – High-severity issues usually put a large number of users' sensitive information at risk, or are reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
- **Medium severity** – Medium-severity issues tend to put a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or are reasonably likely to lead to moderate financial impact.
- **Low severity** – 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 post an immediate risk, but is relevant to security best practices or Defence in Depth.
- **Undetermined** – The impact of the issue is uncertain.
- **Fixed** – Adjusted program implementation, requirements or constraints to eliminate the risk.
- **Mitigated** – Implemented actions to minimize the impact or likelihood of the risk.
- **Acknowledged** – The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).

Appendix

File Signatures

The following are the SHA-256 hashes of the reviewed files. A file with a different SHA-256 hash has been modified, intentionally or otherwise, after the security review. You are cautioned that a different SHA-256 hash could be (but is not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of the review.

Files

- d98...a8c ./contracts/interfaces/IApi3ReaderProxy.sol
- 377...6dc ./contracts/api3-server-v1/Api3MarketV2.sol
- 9ac...9be ./contracts/api3-server-v1/BeaconUpdatesWithSignedData.sol
- 699...2e0 ./contracts/api3-server-v1/DapiServer.sol
- 287...495 ./contracts/api3-server-v1/AirseekerRegistry.sol
- 10a...d1c ./contracts/api3-server-v1/OevDataFeedServer.sol
- 9a2...4b7 ./contracts/api3-server-v1/Api3ServerV1OevExtension.sol
- e75...40e ./contracts/api3-server-v1/OevDapiServer.sol
- 41e...2dc ./contracts/api3-server-v1/OevAuctionHouse.sol
- b80...91d ./contracts/api3-server-v1/Api3ServerV1.sol
- e40...849 ./contracts/api3-server-v1/DataFeedServer.sol
- bb7...a96 ./contracts/api3-server-v1/interfaces/IOevDataFeedServer.sol
- fca...e22 ./contracts/api3-server-v1/interfaces/IApi3MarketV2.sol
- 3ca...b32 ./contracts/api3-server-v1/interfaces/IApi3ServerV1.sol
- ac7...1b7 ./contracts/api3-server-v1/interfaces/IOevAuctionHouse.sol
- 168...5fc ./contracts/api3-server-v1/interfaces/IDapiServer.sol
- 89b...050 ./contracts/api3-server-v1/interfaces/IBeaconUpdatesWithSignedData.sol
- 5dd...e57 ./contracts/api3-server-v1/interfaces/IAirseekerRegistry.sol
- a8e...472 ./contracts/api3-server-v1/interfaces/IOevDapiServer.sol
- 889...ea8 ./contracts/api3-server-v1/interfaces/IApi3ServerV1OevExtension.sol
- f63...6aa ./contracts/api3-server-v1/interfaces/IDataFeedServer.sol
- eff...1bf ./contracts/api3-server-v1/proxies/Api3ReaderProxyV1.sol
- 976...829 ./contracts/api3-server-v1/proxies/Api3ReaderProxyV1Factory.sol
- ea7...8a3 ./contracts/api3-server-v1/proxies/interfaces/IApi3ReaderProxyV1Factory.sol
- df5...a3d ./contracts/api3-server-v1/proxies/interfaces/IProxy.sol
- 867...74c ./contracts/api3-server-v1/proxies/interfaces/IOevProxy.sol
- c41...23f ./contracts/api3-server-v1/proxies/interfaces/IApi3ReaderProxyV1.sol
- a7c...697 ./contracts/api3-server-v1/aggregation/Median.sol
- c17...1f0 ./contracts/api3-server-v1/aggregation/QuickSelect.sol
- 4f6...bd4 ./contracts/api3-server-v1/aggregation/Sort.sol
- 81b...289 ./contracts/utils/SelfMulticall.sol
- a0d...81b ./contracts/utils/ExtendedSelfMulticall.sol
- 94e...512 ./contracts/utils/interfaces/IExtendedSelfMulticall.sol
- 74b...dd6 ./contracts/utils/interfaces/ISelfMulticall.sol
- 331...047 ./contracts/access/GnosisSafeWithoutProxy.sol
- f18...6e1 ./contracts/access/AccessControlRegistry.sol
- 191...459 ./contracts/access/AccessControlRegistryAdminnedWithManager.sol
- 7f2...35e ./contracts/access/RoleDeriver.sol
- 04f...428 ./contracts/access/HashRegistry.sol
- 218...4a7 ./contracts/access/OwnableCallForwarder.sol
- 262...3a9 ./contracts/access/AccessControlRegistryAdminned.sol
- c99...c4f ./contracts/access/interfaces/IOwnable.sol
- cfb...740 ./contracts/access/interfaces/IOwnableCallForwarder.sol
- 88d...1b6 ./contracts/access/interfaces/IAccessControlRegistry.sol
- 30c...839 ./contracts/access/interfaces/IHashRegistry.sol
- 3f2...142 ./contracts/access/interfaces/IAccessControlRegistryAdminned.sol
- 79d...9c6 ./contracts/access/interfaces/IAccessControlRegistryAdminnedWithManager.sol

Tests

- 094...980 ./test/test-utils.ts
- cb6...cd2 ./test/api3-server-v1/Api3MarketV2.sol.ts
- d85...a83 ./test/api3-server-v1/OevAuctionHouse.sol.ts
- d38...300 ./test/api3-server-v1/AirseekerRegistry.sol.ts

- `3cf...9f8 ./test/api3-server-v1/Api3ServerV1.sol.ts`
- `a1a...845 ./test/api3-server-v1/Api3ServerV1OevExtension.sol.ts`
- `325...44b ./test/api3-server-v1/proxies/Api3ReaderProxyV1.sol.ts`
- `272...d74 ./test/api3-server-v1/proxies/Api3ReaderProxyV1Factory.sol.ts`
- `378...9f9 ./test/api3-server-v1/aggregation/Median.sol.ts`
- `622...d0c ./test/utils/ExtendedSelfMulticall.sol.ts`
- `d1f...9f4 ./test/utils/SelfMulticall.sol.ts`
- `9c6...1c8 ./test/access/OwnableCallForwarder.sol.ts`
- `3ae...25b ./test/access/HashRegistry.sol.ts`
- `cb7...62e ./test/access/AccessControlRegistryAdminnedWithManager.sol.ts`
- `7a5...dcf ./test/access/AccessControlRegistryAdminned.sol.ts`
- `bec...f87 ./test/access/GnosisSafeWithoutProxy.sol.ts`
- `bd2...c3b ./test/access/AccessControlRegistry.sol.ts`

Automated Analysis

N/A

Test Suite Results

The test suite was run with the following command. All test cases were run successfully.

```
pnpm i && pnpm build
pnpm test:coverage
```

Update: Five tests were added during the fix review. All 446 tests passed.

```
  AccessControlRegistry
    initializeManager
      Manager address is not zero
        Manager is not initialized
          ✔ initializes manager (39ms)
        Manager is initialized
          ✔ does nothing
      Manager address is zero
        ✔ reverts
    renounceRole
      role is not the root role of account
        Sender is account
          account has role
            ✔ renounces role
          account does not have role
            ✔ does nothing
        Sender is not account
          ✔ reverts
      role is the root role of account
        ✔ reverts
  initializeRoleAndGrantToSender
    description is not empty
      Role is not initialized
        adminRole is the root role of the sender
          Sender manager is initialized
            ✔ initializes role and grants it to the sender
          Sender manager is not initialized
            ✔ initializes sender manager, role and grants it to the sender
        adminRole is not the root role of the sender
          Sender has adminRole
            ✔ initializes role and grants it to the sender
          Sender does not have adminRole
            ✔ reverts (49ms)
      Role is initialized
```

```
        Sender has adminRole
          ✔ grants role to sender
        Sender does not have adminRole
          ✔ reverts (45ms)
    description is empty
      ✔ reverts
  multicall
    ✔ multicalls (61ms)
  tryMulticall
    ✔ tries to multicall (99ms)

AccessControlRegistryAdminned
  constructor
    AccessControlRegistry address is not zero
      Admin role description is not empty
        ✔ constructs
      Admin role description is not empty
        ✔ reverts
    AccessControlRegistry address is zero
      ✔ reverts
  multicall
    ✔ multicalls
  tryMulticall
    ✔ tries to multicall

AccessControlRegistryAdminnedWithManager
  constructor
    Manager address is not zero
      ✔ constructs
    Manager address is zero
      ✔ reverts

GnosisSafeWithoutProxy
  constructor
    ✔ sets up the contract (78ms)
  setup
    ✔ reverts
  execTransaction
    Transaction is direct
      Transaction is a function call
        ✔ executes transaction
      Transaction is not a function call
        ✔ executes transaction
    Transaction is through OwnableCallForwarder
      Transaction is a function call
        ✔ executes transaction
  changeThreshold
    ✔ changes threshold
  addOwnerWithThreshold
    ✔ adds owner with threshold

HashRegistry
  constructor
    Owner address is not zero
      ✔ constructs (50ms)
    Owner address is zero
      ✔ reverts
  renounceOwnership
    ✔ renounces ownership
  transferOwnership
    ✔ transfers ownership
  setSigners
    Sender is the owner
      Hash type is not zero
        Signers are not empty
          First signer address is not zero
            Signer addresses are in ascending order
              ✔ sets signers
            Signer addresses are not in ascending order
              ✔ reverts
          First signer address is zero
            ✔ reverts
```

```
      Signers are empty
        ✔ reverts
    Hash type is zero
      ✔ reverts
  Sender is not the owner
    ✔ reverts
setHash
  Sender is the owner
    ✔ sets hash (66ms)
  Sender is not the owner
    ✔ reverts
registerHash
  Hash value is not zero
    Timestamp is not from the future
      Timestamp is more recent than the previous one
        Signers are set for the hash type
          No delegation signature is used
            All signatures match
              ✔ registers hash
            Not all signatures match
              ✔ reverts
          Delegation signatures are used
            All signatures have a valid length
              None of the delegation signatures have expired
                All delegate hash signatures are valid
                  All delegation signatures are valid
                    ✔ registers hash
                  Not all delegation signatures are valid
                    ✔ reverts
                Not all delegate hash signatures are valid
                  ✔ reverts
              Some of the delegation signatures have expired
                ✔ reverts
            Not all signatures have a valid length
              ✔ reverts
        Signers are not set for the hash type
          ✔ reverts
      Timestamp is not more recent than the previous one
        ✔ reverts (65ms)
    Timestamp is from the future
      ✔ reverts
  Hash value is not zero
    ✔ reverts

OwnableCallForwarder
  constructor
    ✔ constructor
  forwardCall
    Sender is the owner
      Target address belongs to a contract
        Target function exists
          Target function is payable
            Message value is zero
              Target function does not revert
                ✔ forwards call
              Target function reverts
                ✔ reverts
            Message value is not zero
              Target function does not revert
                ✔ forwards call
              Target function reverts
                ✔ reverts
          Target function is not payable
            Message value is zero
              Target function does not revert
                ✔ forwards call
              Target function reverts
                ✔ reverts
            Message value is not zero
              ✔ reverts
        Target function does not exist
          ✔ reverts
```

```
      Target address does not belong to a contract
        ✔ reverts
    Sender is not the owner
      ✔ reverts

AirseekerRegistry
  constructor
    Owner address is not zero
      Api3ServerV1 address is not zero
        ✔ constructs (95ms)
      Api3ServerV1 address is zero
        ✔ reverts
    Owner address is zero
      ✔ reverts
  renounceOwnership
    ✔ reverts
  transferOwnership
    ✔ reverts
  setDataFeedIdToBeActivated
    Sender is the owner
      Data feed ID is not zero
        Data feed ID is not activated
          ✔ activates the data feed ID
        Data feed ID is already activated
          ✔ does nothing
      Data feed ID is zero
        ✔ reverts
    Sender is not the owner
      ✔ reverts
  setDapiNameToBeActivated
    Sender is the owner
      dAPI name is not zero
        dAPI name is not activated
          ✔ activates the dAPI name
        dAPI name is already activated
          ✔ does nothing
      dAPI name is zero
        ✔ reverts
    Sender is not the owner
      ✔ reverts
  setDataFeedIdToBeDeactivated
    Sender is the owner
      Data feed ID is not zero
        Data feed ID is activated
          ✔ deactivates the data feed ID
        Data feed ID is not activated
          ✔ does nothing
      Data feed ID is zero
        ✔ reverts
    Sender is not the owner
      ✔ reverts
  setDapiNameToBeDeactivated
    Sender is the owner
      dAPI name is not zero
        dAPI name is activated
          ✔ deactivates the dAPI name
        dAPI name is not activated
          ✔ does nothing
      dAPI name is zero
        ✔ reverts
    Sender is not the owner
      ✔ reverts
  setDataFeedIdUpdateParameters
    Sender is the owner
      Data feed ID is not zero
        Update parameters length does not exceed the maximum
          Values update update parameters
            Values have not been used before
              ✔ updates update parameters
            Values have been used before
              ✔ updates update parameters
          Values do not update update parameters
```

```
          ✔ does nothing
        Update parameters length exceeds the maximum
          ✔ reverts
      Data feed ID is zero
        ✔ reverts
    Sender is not the owner
      ✔ reverts
  setDapiNameUpdateParameters
    Sender is the owner
      dAPI name is not zero
        Update parameters length does not exceed the maximum
          Values update update parameters
            Values have not been used before
              ✔ updates update parameters
            Values have been used before
              ✔ updates update parameters
          Values do not update update parameters
            ✔ does nothing
        Update parameters length exceeds the maximum
          ✔ reverts
      dAPI name is zero
        ✔ reverts
    Sender is not the owner
      ✔ reverts
  setSignedApiUrl
    Sender is the owner
      Airnode address is not zero
        Signed API URL is not too long
          Value updates signed API URL
            ✔ updates signed API URL
          Value does not update signed API URL
            ✔ does nothing
        Signed API URL is too long
          ✔ reverts
      Airnode address is zero
        ✔ reverts
    Sender is not the owner
      ✔ reverts
  registerDataFeed
    Data feed details are long enough to specify a single Beacon
      Airnode address is not zero
        Data feed is not registered
          ✔ registers data feed
        Data feed is already registered
          ✔ does nothing
      Airnode address is zero
        ✔ reverts
    Data feed details are at least long enough to specify a Beacon set composed of two Beacons
      Data feed details length does not exceed specifications for a Beacon set composed of the maximum
number of Beacons
        Data feed details data does not trail
          Data feed detail parameter lengths match
            None of the Airnode addresses is zero
              Data feed is not registered
                ✔ registers data feed
              Data feed is already registered
                ✔ does nothing
            Some of the Airnode addresses are zero
              ✔ reverts
          Data feed detail parameter lengths do not match
            ✔ reverts
        Data feed details data trail
          ✔ reverts
      Data feed details length exceeds specifications for a Beacon set composed of the maximum number
of Beacons
        ✔ reverts
    Data feed details neither long enough to specify a single Beacon or at least long enough to specify
a Beacon set composed of two Beacons
      ✔ reverts
  activeDataFeed
    The index belongs to an active data feed ID
      Data feed ID update parameters have been set
```

```
          Data feed details have been set
            Data feed is a Beacon set
              ✔ returns data feed ID, details, reading, Beacon readings, update parameters and respective
signed API URLs (47ms)
            Data feed is a Beacon
              ✔ returns data feed ID, details, reading, Beacon reading, update parameters and the
respective signed API URL
          Data feed details have not been set
            ✔ returns data feed ID, reading and update parameters
        Data feed ID update parameters have not been set
          Data feed details have been set
            Data feed is a Beacon set
              ✔ returns data feed ID, details, reading, Beacon readings and respective signed API URLs
(41ms)
            Data feed is a Beacon
              ✔ returns data feed ID, details, reading, Beacon reading and the respective signed API URL
          Data feed details have not been set
            ✔ returns data feed ID and reading
      The index belongs to an active dAPI name
        dAPI name has been set at Api3ServerV1
          dAPI name update parameters have been set
            Data feed details have been set
              Data feed is a Beacon set
                ✔ returns data feed ID, dAPI name, details, reading, Beacon readings, update parameters
and respective signed API URLs (52ms)
              Data feed is a Beacon
                ✔ returns data feed ID, dAPI name, details, reading, Beacon reading, update parameters
and the respective signed API URL
            Data feed details have not been set
              ✔ returns data feed ID, dAPI name, reading and update parameters
          dAPI name update parameters have not been set
            Data feed details have been set
              Data feed is a Beacon set
                ✔ returns data feed ID, dAPI name, details, reading, Beacon readings and respective
signed API URLs (42ms)
              Data feed is a Beacon
                ✔ returns data feed ID, dAPI name, details, reading, Beacon reading and the respective
signed API URL
            Data feed details have not been set
              ✔ returns data feed ID, dAPI name, details, reading and respective signed API URLs
        dAPI name has not been set at Api3ServerV1
          dAPI name update parameters have been set
            ✔ returns dAPI name and update parameters
          dAPI name update parameters have not been set
            ✔ returns dAPI name
      The index does not belong to an active data feed ID or dAPI name
        ✔ returns nothing

Api3MarketV2
  constructor
    Maximum subscription queue length is not zero
      ProxyFactory address belongs to a contract with the expected interface
        ✔ constructs (8663ms)
      ProxyFactory address belongs to a contract without the expected interface
        ✔ reverts
      ProxyFactory address does not belong to a contract
        ✔ reverts
    Maximum subscription queue length is zero
      ✔ reverts
  renounceOwnership
    ✔ reverts
  transferOwnership
    ✔ reverts
  setAirseekerRegistry
    Sender is the owner
      AirseekerRegistry address is not zero
        AirseekerRegistry address is not set yet
          AirseekerRegistry owner is Api3MarketV2
            ✔ sets AirseekerRegistry address
          AirseekerRegistry owner is not Api3MarketV2
            ✔ reverts
        AirseekerRegistry address is already set
```

```
        ✔ reverts
    AirseekerRegistry address is zero
      ✔ reverts
  Sender is not the owner
    ✔ reverts
buySubscription
  Arguments are valid
    New subscription can be added to the queue
      Payment is enough to get the sponsor wallet balance over the expected amount
        Payment amount is not zero
          Payment transfer succeeds
            Subscription is added to the start of the queue
              dAPI name needs to be updated
                ✔ updates dAPI name and buys subscription (131ms)
              dAPI name does not need to be updated
                ✔ buys subscription (266ms)
            Subscription is not added to the start of the queue
              Current subscription ID does not need to be updated
                dAPI name needs to be updated
                  ✔ updates dAPI name and buys subscription (194ms)
                dAPI name does not need to be updated
                  ✔ buys subscription (181ms)
              Current subscription ID needs to be updated
                dAPI name needs to be updated
                  ✔ updates current subscription ID, updates dAPI name and buys subscription (317ms)
                dAPI name does not need to be updated
                  ✔ updates current subscription ID and buys subscription (308ms)
          Payment transfer fails
            ✔ reverts (172ms)
        Payment amount is zero
          ✔ buys subscription (181ms)
      Payment is not enough to get the sponsor wallet balance over the expected amount
        ✔ reverts (78ms)
    New subscription cannot be added to the queue...
      ...because its deviation reference differs from the subscriptions in the queue
        ✔ reverts (99ms)
      ...because its deviation threshold and heartbeat interval are not comparable to a subscription
in the queue
        ✔ reverts (95ms)
      ...because new subscription does not upgrade the queue
        ✔ reverts (90ms)
      ...because the queue is full
        ✔ reverts (342ms)
      ...because doing so will result in a dAPI name to be set to a stale data feed
        ✔ reverts (73ms)
      ...because doing so will result in a dAPI name to be set to an unregistered data feed
        ✔ reverts (59ms)
      ...because doing so requires Api3MarketV2 to set a dAPI name and Api3MarketV2 does not have the
respective Api3ServerV1 role
        ✔ reverts (82ms)
    Arguments are not valid
      Data feed ID is zero
        ✔ reverts
      Sponsor wallet address is zero
        ✔ reverts
      dAPI management Merkle proof verification is not successful...
        ...because dAPI name is zero
          ✔ reverts
        ...because dAPI management Merkle data cannot be decoded
          ✔ reverts
        ...because dAPI management Merkle root is not registered
          ✔ reverts
        ... dAPI management Merkle proof is not valid
          ✔ reverts
      dAPI pricing Merkle proof verification is not successful...
        ...because update parameters length is invalid
          ✔ reverts
        ...because duration is zero
          ✔ reverts
        ...because price is zero
          ✔ reverts
        ...because dAPI pricing Merkle data cannot be decoded
```

```
        ✔ reverts
      ...because dAPI pricing Merkle root is not registered
        ✔ reverts
      ... dAPI pricing Merkle proof is not valid
        ✔ reverts
cancelSubscriptions
  Sender is the owner
    dAPI subscription queue is not empty
      ✔ cancels subscriptions (138ms)
    dAPI subscription queue is empty
      ✔ reverts
  Sender is not the owner
    ✔ reverts
updateCurrentSubscriptionId
  dAPI subscription queue is not empty
    Current subscription ID needs to be updated
      Queue will be empty after the current subscription ID is updated
        ✔ updates the current subscription ID and deactivates the dAPI (207ms)
      Queue will not be empty after the current subscription ID is updated
        ✔ updates the subscription ID and updates the update parameters (215ms)
    Current subscription ID does not need to be updated
      ✔ reverts (75ms)
  dAPI subscription queue is empty
    ✔ reverts
updateDapiName
  Arguments are valid
    Data feed ID is different than what the dAPI name is currently set to
      Sets the dAPI name to a non-zero data feed ID
        Data feed is ready
          ✔ updates dAPI name (39ms)
        Data feed is not ready
          Data feed is stale
            ✔ reverts (64ms)
          Data feed has not been registered
            ✔ reverts
      Sets the dAPI name to zero data feed ID
        ✔ updates dAPI name (46ms)
    Data feed ID is not different than what the dAPI name is currently set to
      ✔ reverts (42ms)
  Arguments are not valid
    Sponsor wallet address is zero while data feed ID is not
      ✔ reverts
    Data feed ID is zero while sponsor wallet address is not
      ✔ reverts
    dAPI management Merkle proof verification is not successful...
      ...because dAPI name is zero
        ✔ reverts
      ...because dAPI management Merkle data cannot be decoded
        ✔ reverts
      ...because dAPI management Merkle root is not registered
        ✔ reverts
      ... dAPI management Merkle proof is not valid
        ✔ reverts
updateSignedApiUrl
  Signed API URL Merkle proof verification is successful
    Signed API URL is different than that the signed API URL is currently set to
      ✔ updates signed API URL
    Signed API URL is not different than that the signed API URL is currently set to
      ✔ reverts (38ms)
  Signed API URL Merkle proof verification is not successful...
    ...because signed API URL Merkle data cannot be decoded
      ✔ reverts
    ...because signed API URL Merkle root is not registered
      ✔ reverts
    ... signed API URL Merkle proof is not valid
      ✔ reverts
API3 Market flow
  ✔ works as intended (547ms)
updateBeaconWithSignedData
  ✔ updates Beacon with signed data
updateBeaconSetWithBeacons
  ✔ updates Beacon set with Beacons
```

```
deployApi3ReaderProxyV1
  ✔ deploys Api3ReaderProxyV1 (39ms)
registerDataFeed
  ✔ registers data feed
computeExpectedSponsorWalletBalance
  ✔ computes expected sponsor wallet balance (186ms)
computeExpectedSponsorWalletBalanceAfterSubscriptionIsAdded
  Update parameters length is valid
    ✔ computes expected sponsor wallet balance after subscription is added (133ms)
  Update parameters length is invalid
    ✔ reverts (113ms)
getDapiData
  dAPI name is set to a Beacon set
    ✔ gets dAPI data (209ms)
  dAPI name is set to a Beacon
    ✔ gets dAPI data (191ms)
getDataFeedData
  Data feed ID belongs to a Beacon set
    ✔ gets data feed data
  Data feed ID belongs to a Beacon
    ✔ gets data feed data
subscriptionIdToUpdateParameters
  Subscription exists
    ✔ returns the update parameters of the subscription (64ms)
  Subscription does not exist
    ✔ returns empty bytes string

Api3ServerV1
  constructor
    ✔ constructs (94ms)
  updateBeaconSetWithBeacons
    Did not specify less than two Beacons
      Beacons update Beacon set timestamp
        ✔ updates Beacon set (120ms)
      Beacons do not update Beacon set timestamp
        Beacons update Beacon set value
          ✔ updates Beacon set (142ms)
        Beacons do not update Beacon set value
          ✔ reverts (151ms)
    Specified less than two Beacons
      ✔ reverts (91ms)
  updateBeaconWithSignedData
    Timestamp is valid
      Signature is valid
        Fulfillment data length is correct
          Decoded fulfillment data can be typecasted into int224
            Updates timestamp
              ✔ updates Beacon with signed data (87ms)
            Does not update timestamp
              ✔ reverts (102ms)
          Decoded fulfillment data cannot be typecasted into int224
            ✔ reverts (103ms)
        Fulfillment data length is not correct
          ✔ reverts (91ms)
      Signature is not valid
        ✔ reverts (85ms)
  Timestamp is more than 1 hour from the future
    ✔ reverts (81ms)
  Timestamp is zero
    ✔ reverts (82ms)
updateOevProxyDataFeedWithSignedData
  Timestamp is valid
    Updates timestamp
      Fulfillment data length is correct
        Decoded fulfillment data can be typecasted into int224
          More than one Beacon is specified
            There are no invalid signatures
              There are enough signatures to constitute an absolute majority
                Data in packed signatures is consistent with the data feed ID
                  ✔ updates OEV proxy Beacon set with signed data (107ms)
                Data in packed signatures is not consistent with the data feed ID
                  ✔ reverts (112ms)
```

```
            There are not enough signatures to constitute an absolute majority
              ✔ reverts (100ms)
            There are invalid signatures
              ✔ reverts (84ms)
          One Beacon is specified
            The signature is not invalid
              The signature is not omitted
                Data in the packed signature is consistent with the data feed ID
                  ✔ updates OEV proxy Beacon with signed data (99ms)
                Data in the packed signature is not consistent with the data feed ID
                  ✔ reverts (89ms)
              The signature is omitted
                ✔ reverts (85ms)
            The signature is invalid
              ✔ reverts (89ms)
          No Beacon is specified
            ✔ reverts (80ms)
        Decoded fulfillment data cannot be typecasted into int224
          ✔ reverts (88ms)
      Fulfillment data length is not correct
        ✔ reverts (81ms)
    Does not update timestamp
      ✔ reverts (96ms)
  Timestamp is more than 1 hour from the future
    ✔ reverts (113ms)
  Timestamp is zero
    ✔ reverts (83ms)
withdraw
  OEV proxy announces a beneficiary address
    OEV proxy announces a non-zero beneficiary address
      OEV proxy balance is not zero
        Beneficiary does not revert the transfer
          ✔ withdraws the OEV proxy balance to the respective beneficiary (94ms)
        Beneficiary reverts the transfer
          ✔ reverts (94ms)
      OEV proxy balance is zero
        ✔ reverts (80ms)
    OEV proxy announces a zero beneficiary address
      ✔ reverts (79ms)
  OEV proxy does not announce a beneficiary address
    ✔ reverts (80ms)
setDapiName
  dAPI name is not zero
    Data feed ID is not zero
      Sender is manager
        ✔ sets dAPI name (91ms)
      Sender is dAPI name setter
        ✔ sets dAPI name (103ms)
      Sender is not dAPI name setter
        ✔ reverts (91ms)
    Data feed ID is zero
      Sender is manager
        ✔ sets dAPI name (109ms)
      Sender is dAPI name setter
        ✔ sets dAPI name (145ms)
      Sender is not dAPI name setter
        ✔ reverts (125ms)
  dAPI name is zero
    ✔ reverts (129ms)
readDataFeedWithId
  Data feed is initialized
    ✔ reads data feed (95ms)
  Data feed is not initialized
    ✔ reverts (100ms)
readDataFeedWithDapiNameHash
  dAPI name set to Beacon
    Data feed is initialized
      ✔ reads Beacon (90ms)
    Data feed is not initialized
      ✔ reverts (89ms)
  dAPI name set to Beacon set
    Data feed is initialized
```

```
      ✔ reads Beacon set (123ms)
    Data feed is not initialized
      ✔ reverts (82ms)
  dAPI name not set
    ✔ reverts (84ms)
readDataFeedWithIdAsOevProxy
  Data feed is initialized
    OEV proxy data feed is more up to date
      ✔ reads OEV proxy data feed (89ms)
    Base data feed is more up to date
      ✔ reads base data feed (93ms)
  Data feed is not initialized
    ✔ reverts (98ms)
readDataFeedWithDapiNameHashAsOevProxy
  dAPI name set to Beacon
    Data feed is initialized
      OEV proxy data feed is more up to date
        ✔ reads OEV proxy data feed (99ms)
      Base data feed is more up to date
        ✔ reads base data feed (91ms)
    Data feed is not initialized
      ✔ reverts (86ms)
  dAPI name set to Beacon set
    Data feed is initialized
      OEV proxy data feed is more up to date
        ✔ reads OEV proxy data feed (126ms)
      Base data feed is more up to date
        ✔ reads base data feed (130ms)
    Data feed is not initialized
      ✔ reverts (93ms)
  dAPI name not set
    ✔ reverts (86ms)

Api3ServerV1OevExtension
  constructor
    Api3ServerV1 address is not zero
      ✔ constructs (131ms)
    Api3ServerV1 address is zero
      ✔ reverts
  withdraw
    Recipient is not zero address
      Amount is not zero
        Sender is the manager
          Withdrawal is successful
            ✔ withdraws
          Withdrawal is not successful
            ✔ reverts
        Sender is a withdrawer
          Withdrawal is successful
            ✔ withdraws
          Withdrawal is not successful
            ✔ reverts
        Sender is not the manager or a sender
          ✔ reverts
      Amount is zero
        ✔ reverts
    Recipient is zero address
      ✔ reverts
payOevBid
  dApp ID is not zero
    Timestamp is not zero
      Timestamp is not too far from the future
        Signature is valid
          Last paid bid timestamp cut-off is more recent than the current one
            ✔ pays OEV bid
          Last paid bid timestamp cut-off is not more recent than the current one
            ✔ reverts
        Signature is not valid
          ✔ reverts
      Timestamp is too far from the future
        ✔ reverts
    Timestamp is zero
```

```
      ✔ reverts
  dApp ID is zero
    ✔ reverts
updateDappOevDataFeed
  Sender is the last bid payer for the dApp
    Signed data is not empty
      Signed data has a single item
        Signature is valid
          Timestamp is smaller than or equal to the cut-off
            Timestamp updates
              ✔ updates dApp OEV data feed
            Timestamp does not update
              ✔ reverts
          Timestamp is larger than the cut-off
            ✔ reverts
        Signature is not valid
          ✔ reverts
      Signed data has multiple items
        No signature has been omitted
          All signatures are valid
            All timestamps are smaller than or equal to the cut-off
              All timestamps update
                All timestamps are larger than the base counterparts
                  Updates OEV Beacon set timestamp
                    ✔ updates dApp OEV data feed (65ms)
                  Does not update OEV Beacon set timestamp
                    Updates OEV Beacon set value
                      ✔ updates dApp OEV data feed (114ms)
                    Does not update OEV Beacon set value
                      ✔ reverts (132ms)
                Not all timestamps are larger than the base counterparts
                  ✔ updates dApp OEV data feed by using base Beacon values as necessary (86ms)
              Not all timestamps update
                ✔ reverts (65ms)
            Some timestamps are larger than the cut-off
              ✔ reverts
          Not all signatures are valid
            ✔ reverts (51ms)
        Some signatures have been omitted
          ✔ updates dApp OEV data feed (170ms)
    Signed data is empty
      ✔ reverts (163ms)
  Sender is not the last bid payer for the dApp
    ✔ reverts
simulateDappOevDataFeedUpdate
  Sender impersonates zero address
    Sender static-calls
      ✔ simulates dApp OEV data feed update
    Sender does not impersonate zero address
      Sender static-calls
        ✔ reverts
      Sender calls
        ✔ reverts
  simulateExternalCall
    Sender impersonates zero address
      Sender static-calls
        ✔ simulates external call (39ms)
    Sender does not impersonate zero address
      Sender static-calls
        ✔ reverts
      Sender calls
        ✔ reverts

OevAuctionHouse
  constructor
    ✔ constructs (92ms)
  setCollateralInBasisPoints
    Sender is the manager
      ✔ sets collateral requirement in basis points
    Sender is not the manager
      ✔ reverts
  setProtocolFeeInBasisPoints
```

```
    Sender is the manager
      ✔ sets protocol fee in basis points
    Sender is not the manager
      ✔ reverts
  setCollateralRateProxy
    Sender is a proxy setter
      Collateral rate proxy address is not zero
        ✔ sets collateral rate proxy
      Collateral rate proxy address is zero
        ✔ reverts
    Sender is the manager
      Collateral rate proxy address is not zero
        ✔ sets collateral rate proxy
      Collateral rate proxy address is zero
        ✔ reverts
    Sender is not a proxy setter or the manager
      ✔ reverts
  setChainNativeCurrencyRateProxy
    Sender is a proxy setter
      Chain ID is not zero
        Collateral rate proxy address is not zero
          ✔ sets collateral rate proxy
        Collateral rate proxy address is zero
          ✔ reverts
      Chain ID is zero
        ✔ reverts
    Sender is the manager
      Chain ID is not zero
        Collateral rate proxy address is not zero
          ✔ sets collateral rate proxy
        Collateral rate proxy address is zero
          ✔ reverts
      Chain ID is zero
        ✔ reverts
    Sender is not a proxy setter or the manager
      ✔ reverts
  withdrawAccumulatedSlashedCollateral
    Sender is a withdrawer
      Recipient address is not zero
        Amount is not zero
          Amount does not exceed balance
            Transfer is successful
              ✔ withdraws accumulated slashed collateral (302ms)
            Transfer is not successful
              ✔ reverts
          Amount exceeds balance
            ✔ reverts
        Amount is zero
          ✔ reverts
      Recipient address is zero
        ✔ reverts
    Sender is the manager
      Recipient address is not zero
        Amount is not zero
          Amount does not exceed balance
            Transfer is successful
              ✔ withdraws accumulated slashed collateral
            Transfer is not successful
              ✔ reverts
          Amount exceeds balance
            ✔ reverts
        Amount is zero
          ✔ reverts
      Recipient address is zero
        ✔ reverts
    Sender is not a withdrawer or the manager
      ✔ reverts
  withdrawAccumulatedProtocolFees
    Sender is a withdrawer
      Recipient address is not zero
        Amount is not zero
          Amount does not exceed balance
```

```
          Transfer is successful
            ✔ withdraws accumulated protocol fees (428ms)
          Transfer is not successful
            ✔ reverts
        Amount exceeds balance
          ✔ reverts
      Amount is zero
        ✔ reverts
    Recipient address is zero
      ✔ reverts
  Sender is the manager
    Recipient address is not zero
      Amount is not zero
        Amount does not exceed balance
          Transfer is successful
            ✔ withdraws accumulated protocol fees
          Transfer is not successful
            ✔ reverts
        Amount exceeds balance
          ✔ reverts
      Amount is zero
        ✔ reverts
    Recipient address is zero
      ✔ reverts
    Sender is not a withdrawer or the manager
      ✔ reverts
  depositForBidder
    Bidder address is not zero
      Deposit amount is not zero
        ✔ deposits for bidder
      Deposit amount is zero
        ✔ reverts
    Bidder address is zero
      ✔ reverts
  deposit
    Deposit amount is not zero
      ✔ deposits
    Deposit amount is zero
      ✔ reverts
  initiateWithdrawal
    Bidder does not have an initiated withdrawal
      ✔ initiates withdrawal
    Bidder has an initiated withdrawal
      ✔ reverts
  withdraw
    Recipient address is not zero
      Amount is not zero
        Amount does not exceed balance
          Sender has an initiated withdrawal
            It is time for the bidder to be able to withdraw
              Transfer is successful
                ✔ withdraws
              Transfer is not successful
                ✔ reverts
            It is not time yet for the bidder to be able to withdraw
              ✔ reverts
          Sender does not have an initiated withdrawal
            ✔ reverts
        Amount exceeds balance
          ✔ reverts
      Amount is zero
        ✔ reverts
    Recipient address is zero
      ✔ reverts
  cancelWithdrawal
    Sender has an initiated withdrawal
      ✔ cancels the withdrawal
    Sender does not have an initiated withdrawal
      ✔ reverts
  placeBidWithExpiration
    Chain ID is not zero
      Bid amount is not zero
```

```
Bid details length does not exceed the maximum
  Bid details are not empty
    Bid lifetime is not larger than maximum
      Bid lifetime is not shorter than minimum
        Bid is not already placed
          Collateral amount can be calculated
            Maximum collateral amount is not exceeded
              Maximum protocol fee amount is not exceeded
                ✔ places bid with expiration (459ms)
              Maximum protocol fee amount is exceeded
                ✔ reverts (481ms)
            Maximum collateral amount is exceeded
              ✔ reverts (199ms)
          Collateral amount cannot be calculated
            ✔ reverts (497ms)
        Bid is already placed
          ✔ reverts (319ms)
      Bid lifetime is shorter than minimum
        ✔ reverts (88ms)
    Bid lifetime is larger than maximum
      ✔ reverts (86ms)
  Bid details are empty
    ✔ reverts
Bid details length exceeds the maximum
      ✔ reverts
    Bid amount is zero
      ✔ reverts (419ms)
  Chain ID is zero
    ✔ reverts (1408ms)
placeBid
  ✔ places bid (142ms)
expediteBidExpiration
  Bid is awaiting award
    Bid has not expired
      Timestamp expedites bid expiration
        Resulting bid lifetime is not shorter than minimum
          ✔ expedites bid expiration (122ms)
        Resulting bid lifetime is shorter than minimum
          ✔ reverts (977ms)
      Timestamp does not expedite bid expiration
        ✔ reverts (199ms)
    Bid has expired
      ✔ reverts (407ms)
  Bid is not awaiting award
    ✔ reverts (360ms)
expediteBidExpirationMaximally
  ✔ expedites bid expiration maximally (77ms)
awardBid
  Sender is an auctioneer
    Award details length does not exceed the maximum
      Award details are not empty
        Award has not expired
          Bid is awaiting award
            Bid has not expired
              Bidder balance is not lower than the larger of collateral and protocol fee amounts
                Collateral amount is larger than protocol fee amount
                  ✔ awards the bid (326ms)
                Collateral amount is not larger than protocol fee amount
                  ✔ awards the bid (756ms)
              Bidder balance is lower than the larger of collateral and protocol fee amounts
                ✔ reverts
            Bid has expired
              ✔ reverts
          Bid is not awaiting award
            ✔ reverts
        Award has expired
          ✔ reverts
      Award details are empty
        ✔ reverts
    Award details length exceeds the maximum
      ✔ reverts
  Sender is not an auctioneer
```

```
    ✔ reverts
reportFulfillment
  Fulfillment details length does not exceed the maximum
    Fulfillment details are not empty
      Bid is awaiting fulfillment report
        Bid has not expired
          ✔ reports fulfillment (205ms)
        Bid has expired
          ✔ reverts
      Bid is not awaiting fulfillment report
        ✔ reverts
    Fulfillment details are not empty
      ✔ reverts
  Fulfillment details length exceeds the maximum
    ✔ reverts
confirmFulfillment
  Sender is an auctioneer
    Bid is awaiting fulfillment confirmation
      Collateral amount is larger than protocol fee amount
        ✔ confirms fulfillment (948ms)
      Collateral amount is not larger than protocol fee amount
        ✔ confirms fulfillment (407ms)
    Bid is not awaiting fulfillment confirmation
      ✔ reverts
  Sender is not an auctioneer
    ✔ reverts
contradictFulfillment
  Sender is an auctioneer
    Bid is awaiting fulfillment confirmation
      Collateral amount is larger than protocol fee amount
        ✔ contradicts fulfillment
      Collateral amount is not larger than protocol fee amount
        ✔ contradicts fulfillment (440ms)
    Bid is not awaiting fulfillment confirmation
      ✔ reverts
  Sender is not an auctioneer
    ✔ reverts
getCurrentCollateralAndProtocolFeeAmounts
  Collateral requirement and protocol fee are not zero
    Collateral rate proxy is valid
      Collateral rate is positive
        Collateral rate is not stale
          Native currency rate proxy is valid
            Native currency rate is positive
              Native currency rate is not stale
                Collateral and protocol fee amounts are small enough to be typecasted to uint104
                  ✔ gets current collateral and protocol fee amounts
                Collateral and protocol fee amounts are not small enough to be typecasted to uint104
                  ✔ revert
              Native currency rate is stale
                ✔ reverts
            Native currency rate is not positive
              ✔ reverts
          Native currency rate proxy is not valid
            ✔ reverts
        Collateral rate is stale
          ✔ reverts
      Collateral rate is not positive
        ✔ reverts
    Collateral rate proxy is not valid
      ✔ reverts
  Collateral requirement and protocol fee are zero
    ✔ returns zero

Median
  median
    Array length is 1–21
      ✔ computes median of randomly shuffled arrays (2518ms)
  average
    x and y are largest positive numbers
      ✔ computes average without overflowing
    x and y are smallest negative numbers
```

```
      ✔ computes average without undeflowing
    With various combinations of x and y
      ✔ computes average (54ms)

Api3ReaderProxyV1
  constructor
    ✔ constructs (76ms)
  initialize
    ✔ reverts
  read
    dAPI name is set
      At least one of base and OEV feeds has been initialized
        OEV feed timestamp is larger
          ✔ reads OEV feed
        OEV feed timestamp is not larger
          ✔ reads base feed
      Both the base and OEV feeds have not been initialized
        ✔ reverts
    dAPI name is not set
      ✔ reverts
  latestAnswer
    ✔ returns proxy value
  latestTimestamp
    ✔ returns proxy value
  latestRound
    ✔ reverts
  getAnswer
    ✔ reverts
  getTimestamp
    ✔ reverts
  decimals
    ✔ returns 18
  description
    ✔ returns empty string
  version
    ✔ returns 4913
  getRoundData
    ✔ reverts
  latestRoundData
    ✔ returns approximated round data

Api3ReaderProxyV1Factory
  constructor
    Api3ServerV1OevExtension address is not zero
      ✔ constructs (75ms)
    Api3ServerV1OevExtension address is zero
      ✔ reverts
  deployApi3ReaderProxyV1
    dAPI name is not zero
      dApp ID is not zero
        Api3ReaderProxyV1 has not been deployed
          ✔ deploys Api3ReaderProxyV1
        Api3ReaderProxyV1 has already been deployed
          ✔ reverts
      dApp ID is zero
        ✔ reverts
    dAPI name is zero
      ✔ reverts
  computeApi3ReaderProxyV1Address
    dAPI name is not zero
      dApp ID is not zero
        ✔ computes Api3ReaderProxyV1 address
      dApp ID is zero
        ✔ reverts
    dAPI name is zero
      ✔ reverts
  Api3ReaderProxyV1 upgrade flow
    ✔ works as intended (76ms)

ExtendedSelfMulticall
  getChainId
    ✔ gets chain ID
```

```
    containsBytecode
      ✔ returns if account contains bytecode
    getBalance
      ✔ gets balance
    getBlockNumber
      ✔ gets block number
    getBlockTimestamp
      ✔ gets block timestamp
    getBlockBasefee
      ✔ gets block basefee

  SelfMulticall
    multicall
      None of the calls reverts
        ✔ multicall does not revert
      One of the calls reverts
        Call reverts with string
          ✔ multicall reverts by bubbling up the revert string
        Call reverts with custom error
          ✔ multicall reverts by bubbling up the custom error
        Call reverts with no data
          ✔ multicall reverts with no data
    tryMulticall
      None of the calls reverts
        ✔ multicall does not revert
      One of the calls reverts
        Call reverts with string
          ✔ multicall does not revert
        Call reverts with custom error
          ✔ multicall does not revert
        Call reverts with no data
          ✔ multicall does not revert


  441 passing (37s)
```

Code Coverage

Test coverage was obtained by running the following commands.

```
pnpm i && pnpm build
pnpm test:coverage
```

Update: Test coverage remained the same after the fix review.

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
access/	100	100	100	100	
AccessControlRegistry.sol	100	100	100	100	
AccessControlRegistryAdminned.sol	100	100	100	100	
AccessControlRegistryAdminnedWithManager.sol	100	100	100	100	
GnosisSafeWithoutProxy.sol	100	100	100	100	
HashRegistry.sol	100	100	100	100	

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
OwnableCallForwarder.sol	100	100	100	100	
RoleDeriver.sol	100	100	100	100	
access/interfaces/	100	100	100	100	
IAccessControlRegistry.sol	100	100	100	100	
IAccessControlRegistryAdminned.sol	100	100	100	100	
IAccessControlRegistryAdminnedWithManager.sol	100	100	100	100	
IHashRegistry.sol	100	100	100	100	
IOwnable.sol	100	100	100	100	
IOwnableCallForwarder.sol	100	100	100	100	
api3-server-**v1/**	100	100	100	100	
AirseekerRegistry.sol	100	100	100	100	
Api3MarketV2.sol	100	100	100	100	
Api3ServerV1.sol	100	100	100	100	
Api3ServerV1OevExtension.sol	100	100	100	100	
BeaconUpdatesWithSignedData.sol	100	100	100	100	
DapiServer.sol	100	100	100	100	
DataFeedServer.sol	100	100	100	100	
OevAuctionHouse.sol	100	100	100	100	
OevDapiServer.sol	100	100	100	100	
OevDataFeedServer.sol	100	100	100	100	
api3-server-**v1/aggregation/**	99.27	95	100	99.38	
Median.sol	100	100	100	100	
QuickSelect.sol	95.24	92.86	100	97.62	120
Sort.sol	100	95	100	100	
api3-server-**v1/interfaces/**	100	100	100	100	
IAirseekerRegistry.sol	100	100	100	100	
IApi3MarketV2.sol	100	100	100	100	

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
IApi3ServerV1.sol	100	100	100	100	
IApi3ServerV1OevExtension.sol	100	100	100	100	
IBeaconUpdatesWithSignedData.sol	100	100	100	100	
IDapiServer.sol	100	100	100	100	
IDataFeedServer.sol	100	100	100	100	
IOevAuctionHouse.sol	100	100	100	100	
IOevDapiServer.sol	100	100	100	100	
IOevDataFeedServer.sol	100	100	100	100	
api3-server-**v1/proxies/**	100	100	100	100	
Api3ReaderProxyV1.sol	100	100	100	100	
Api3ReaderProxyV1Factory.sol	100	100	100	100	
api3-server-**v1/proxies/interfaces/**	100	100	100	100	
IApi3ReaderProxyV1.sol	100	100	100	100	
IApi3ReaderProxyV1Factory.sol	100	100	100	100	
IOevProxy.sol	100	100	100	100	
IProxy.sol	100	100	100	100	
interfaces/	100	100	100	100	
IApi3ReaderProxy.sol	100	100	100	100	
utils/	93.33	100	87.5	96	
ExtendedSelfMulticall.sol	83.33	100	83.33	83.33	54
SelfMulticall.sol	100	100	100	100	
utils/interfaces/	100	100	100	100	
IExtendedSelfMulticall.sol	100	100	100	100	
ISelfMulticall.sol	100	100	100	100	
All files	99.68	99.64	99.42	99.78	

Changelog

- 2024-10-16 - Initial report
- 2024-10-24 - Final report

About Quantstamp

Quantstamp is a global leader in blockchain security. Founded in 2017, Quantstamp's mission is to securely onboard the next billion users to Web3 through its best-in-class Web3 security products and services.

Quantstamp's team consists of cybersecurity experts hailing from globally recognized organizations including Microsoft, AWS, BMW, Meta, and the Ethereum Foundation. Quantstamp engineers hold PhDs or advanced computer science degrees, with decades of combined experience in formal verification, static analysis, blockchain audits, penetration testing, and original leading-edge research.

To date, Quantstamp has performed more than 500 audits and secured over $200 billion in digital asset risk from hackers. Quantstamp has worked with a diverse range of customers, including startups, category leaders and financial institutions. Brands that Quantstamp has worked with include Ethereum 2.0, Binance, Visa, PayPal, Polygon, Avalanche, Curve, Solana, Compound, Lido, MakerDAO, Arbitrum, OpenSea and the World Economic Forum.

Quantstamp's collaborations and partnerships showcase our commitment to world-class research, development and security. We're honored to work with some of the top names in the industry and proud to secure the future of web3.

Notable Collaborations & Customers:

- Blockchains: Ethereum 2.0, Near, Flow, Avalanche, Solana, Cardano, Binance Smart Chain, Hedera Hashgraph, Tezos
- DeFi: Curve, Compound, Maker, Lido, Polygon, Arbitrum, SushiSwap
- NFT: OpenSea, Parallel, Dapper Labs, Decentraland, Sandbox, Axie Infinity, Illuvium, NBA Top Shot, Zora
- Academic institutions: National University of Singapore, MIT