API Builder Tools 2.0.3 Release Note

> ⚠ **API Builder 3.x is deprecated**
> Support for API Builder 3.x ceased on 30 April 2020. Use the v3 to v4 upgrade guide to migrate all your applications to API Builder 4.x.
>
> Contact support@axway.com if you require migration assistance.

API Builder Tools 2.0.3 - 5 December 2018

API Builder Tools 2.0.3 is a patch release that includes a security fix, a bug fix, and several known issues.

As of this release, the previous API Builder Tools 2.x patch release is no longer supported. End of support for this version will be 2019-12-05 or until the next patch release. Note: Major and minor releases continue to be supported according to their nominal lifetime. See Axway Appcelerator Deprecation Policy and Nominal Lifetimes documents for details.

Fixed security issue

- Previously, an application built with API Builder could allow a remote attacker to bypass authentication to an API endpoint. The issue was discovered by Axway and we have no indications that the vulnerability has been exploited or publicly disclosed. Now, the authentication bypass vulnerability has been resolved in API Builder 2.x.
  - **Summary**: An application built with API Builder could allow a remote attacker to bypass authentication to an API endpoint. The issue was discovered by Axway and we have no indications that the vulnerability has been exploited or publicly disclosed.
  - **Vulnerability details**: An application built with API Builder could allow a remote attacker to bypass authentication to an API endpoint and obtain sensitive information, affect the integrity and availability when using the following authentication mechanisms:
    - HTTP Basic Authentication
    - API Key based Authentication
    - LDAP Authentication
  - **CVSS base score**: 10
  - **CVSS vector**: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N)
  - **Applying remediation/fixes**: If your published applications are using any of the following authentication mechanisms, it is recommended that you download the patch versions and republish your applications:
    - HTTP Basic Authentication
    - API Key based Authentication
    - LDAP Authentication

    For API Builder Applications developed and published with **API Builder 2.x**, download CLI Version 6.3.1 and republish the application using the following steps:
    1. **appc use 6.3.1**
    2. **cd <your project folder>**
    3. **appc publish -f**
  - **Further information**: For additional questions, contact support@axway.com .

Fixed issue

- Previously, a regression update introduced an issue that prevented the inner join queries from working properly. Now, the regression has been fixed and the inner join queries return the expected number of records.

Known issues

- The static config is not refreshed when the configuration is updated.
- Expanding lists causes the page view to jump down.
- If a composite model is loaded from the filesystem where the parent model is stored, then the source of this model is shown as: "user" - "left join with user". This subtext should be removed if the model is the parent.
- The generated endpoint Swagger document has the wrong consumes.
- The legacy distinct() APIs have inconsistent and non-compliant return types.
- The Swagger API and endpoint exports lose their version, name, and description in the exported Swagger documents.
- Clicking on joined models in the *Source* column on the **Models** tab of the API Builder Console does not work. The details of the joined model should be displayed.
- Arrow Swagger exports are not validated with `api-lint`.
- The Arrow `swaggerGenerator` returns a hard-coded `consumes/produces` json and that can't be corrected or customized. The Arrow `swaggerGenerator` also returns hard-coded `ResponseModel` and `ErrorModel` which cannot be removed.
- The `server.addBlock` function does not work.
- Storing relatively large objects in the `req.session` causes Arrow to generate an object to large be stored in a session cookie. The `clie`

`nt-sessions` module encrypts the session object and sets it as a cookie value. However, the object is too large to fit in a cookie, thus the browser never sets it and the following requests use an old cookie, containing an irrelevant session.