

Remarks

Release notes with changes since version 5.3.15.

Upgrade Notes:

Starting with version 5.3.16, 6.1.10, and 6.2.3, Appway will have a security mechanism to protect against "clickjacking" attacks. Appway will no longer allow other web applications (e.g. SharePoint) to embed Appway pages in an <iframe>.

If you have a solution which is integrated in a third-party web application this way you can disable this new security feature by setting the configuration property "nm.security.http.contentpolicy" to "false". Be aware that this will make your solution vulnerable to clickjacking attacks again.

Appway solutions relying on an <iframe> to embed one of its own pages or to embed pages of third-party web applications are not affected by this change.

Links:

<https://www.owasp.org/index.php/Clickjacking>

Appway Platform (Core)

Change

Area	Importance	Description
Security	High	Implementation of a security mechanism against "clickjacking" attacks. Every HTTP response generated by Appway contains the HTTP headers "X-Frame-Options: SAMEORIGIN" and "Content-Security-Policy: frame-ancestors 'self'". These headers instruct browsers to not allow other web applications to embed Appway pages in an iframe. If a solution relies on the integration of Appway pages in a third-party web application, the new configuration property "nm.security.http.contentpolicy" can be set to "false" to disable the inclusion of those HTTP headers.

Bugfix

Area	Importance	Description
DataTable	Low	Using an HTML id with the characters colon (":") and period (".") is now possible.
Screen Components	Low	Dropdown List: Prevent "Uncaught TypeError: Cannot read property 'init' of undefined" when rendering a Dropdown List in an Ajax Update Area.