OM SDK Web (omweb.js) post message vulnerability allowing to execute JavaScript code

Affected Version

The vulnerability has been discovered in the OM SDK Web library (omweb-js) version 1.3.31 and below.

Impact

A XSS vulnerability has been discovered in some configurations omweb-js where post messages can be constructed to cause arbitrary scripts to run on a publisher domain.

The vulnerable scenario appears to be where OM web service and the session client JS are in the top window, and therefore use direct communication rather than post messaging. In this instance, the post messaging listener remains active and may accept messages that don't originate from the session client.

Patches

The problem has been recognized and we are working on a patch. The fix will be available in omweb-js 1.3.32.

Workaround

While we are working on a patch for OM SDK Web, there is a workaround that can be applied depending on the level of urgency.

The OM web service script (omweb-v1.js) can be isolated in an <iframe> (see the following link for details).

https://interactiveadvertisingbureau.github.io/Open-Measurement-SDKJS/iframes.html

Such a setup would avoid this particular injection attack, because the AdSession constructor will send an initial "setup" message, which captures the message source prior to injecting any verification scripts. This provides an additional element of security to avoid injecting any unwanted scripts.

Please be assured we are working to address this issue in all configurations as quickly as possible.

Email us at omsdksupport@iabtechlab.com if you have any questions or comments about this advisory.