2020-05-29 Registry Advisory

The exposure from this vulnerability is expected to be low, and it is unlikely that this vulnerability has been exploited.

Summary

An XSS vulnerability has been announced in jQuery, a JavaScript library used by COmanage Registry. Library versions earlier than 3.5.0 are affected, which means all versions of Registry prior to 3.2.5 are likely to be affected.

Severity

Based on the jQuery announcement, the severity of this vulnerability is unknown. The severity may further vary according to a given deployment pattern.

Exposure

The exposure from this vulnerability is expected to be low, and it is unlikely that this vulnerability has been exploited.

Recommended Mitigation

Upgrade to COmanage Registry v3.2.5 or later.

Deployments using the *develop* branch may pull the latest code from that branch.

Alternate Mitigations

It is possible to manually backport the patch to earlier versions. The diff against v3.2.4 is available here, though the changes may need to be manually applied to older versions.

Discussion

The jQuery.htmlPrefilter() method used for jQuery manipulation methods used regex in versions prior to 3.5.0 that could introduce a cross-site scripting (XSS) vulnerability.

jQuery methods such as .text() and .html() are used in COmanage for manipulating some elements in a rendered View and for generating the content of dialog boxes. While in general text passed to these methods contains no user input, some text passed to dialog boxes may contain usernames or identifiers. Although the nature of this vulnerability is not fully described in the jQuery release notes, it is conceivable that a carefully constructed string entered by a user could trigger the vulnerability. While the COmanage developers do not believe it is likely that this vulnerability has been exploited or is likely to be easily exploited, upgrading as soon as practical is strongly recommended.

References

- CO-1929