Qlik Sense apps can be deleted through API end-point

Qlik bug ID: QLIK-51468

Published: 2016-03-15

Updated: -

Risk rating: Medium

Executive Summary

A vulnerability has been identified in the Qlik API, where a specific API end-point could be leveraged into deleting a published Qlik Sense app.

Affected Software

All Qlik Sense releases prior to Qlik Sense 2.0.8 and Qlik Sense 2.2.4 are affected.

Severity Rating

The vulnerability identified in the API is rated as a medium risk, as the vulnerability requires the attacker to be authenticated to the system, and to know the GUID of the app to delete it. Qlik has rated the vulnerability using the CVSS scoring system. The score, as calculated by Qlik is: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:N/A:H/E:F/RL:O/RC:C

Due to the variable nature of the environments in which Qlik can be deployed, the environment score of the CVSS has not been taken into account. Customers are recommended to assess the risk based on their deployment, and derive a risk rating that is applicable to their deployment. Assessment can be done using the online CVSS scoring system at https://www.first.org/cvss/calculator/3.0.

Vulnerability Details

An API end-point has proven to be vulnerable to an attack where it's possible to delete a published app from a stream. The attacker would have to be authenticated and either be authorized to access the API explorer, or utilize a 3rd party application to be able to talk to the API endpoint directly. The attacker also has to know the GUID of the app that is to be deleted. To exploit the vulnerability, the attacker needs to construct a custom API end-point request.

Recommendation

Customers are recommended to upgrade their Qlik Sense deployment to remediate this vulnerability.

150 N. Radnor Chester Road
Suite E120
Radnor, PA 19087
Phone: +1 (888) 828-9768
Fax: +1 (610) 975-5987

qlik.com