File connector can be modified through API end-point

Qlik bug ID: QLIK-51470

Published: 2016-03-15

Updated: -

Risk rating: Medium

Executive Summary

A vulnerability has been identified in the Qlik Sense API, where a specific API end-point can be used to change the local folder connector which is used for end users to be able to upload data to servers and load data into their apps.

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 is rated as medium, as the vulnerability requires the attacker to be authenticated to the system, to gain read access to the local file system on the server hosting the Qlik Sense deployment. 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:H/I:N/A:N/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

Qlik Sense offers authenticated users the ability to attach files while developing apps though a pre-configured file connector. This allows the user an easy way of analyzing their data. An end-point in the Qlik Sense API has proven itself vulnerable to an attack, where the file connector is modified in such a way that an attacker can redirect it to any folder in the filesystem of the server hosting Qlik Sense, which Qlik Sense has read access to. Files that Qlik Sense can parse can then be read by the attacker within the context of a Qlik Sense app.

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. 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