



Local filesystem access through API endpoint

Qlik bug ID: QLIK-51361

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 enumerating files and folders stored locally on the server where Qlik Sense was installed. In certain scenarios the content of the files could be disclosed.

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 it could be leveraged into disclosing information about the local filesystem of the server Qlik Sense was hosted on. Adding to the rating is the scenario where the content of the files could be disclosed. Qlik has rated the vulnerability using the CVSS scoring system. The score, as calculated by Qlik is: CVSS:3.0/AV:N/AC:L/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

An API end-point has proven to be vulnerable to an attack where it's possible to disclose information regarding local files and folders on the server hosting Qlik Sense. Depending on the file-type, the content of the file could also be disclosed.

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

