XSS vulnerability in the QMC node overview page

Qlik bug ID: QLIK-51134

Published: 2016-03-15

Updated: -

Risk rating: Medium

Executive Summary

A vulnerability has been identified in the Qlik Management Console, where a specific input field has proven itself to be susceptible to a Cross Site Scripting (XSS) attack.

Affected Software

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

Severity Rating

The XSS vulnerability identified in the QMC is rated as medium. This is based on the risk of non-Qlik code being executed on the client, limited by the requirement of having specific administrator authorization in the QMC. 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:H/UI:R/S:C/C:L/I:L/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

The XSS vulnerability was found in the handling of the input-data as part of adding a new node to the system and giving it name. To successfully exploit this vulnerability, the attacker would need Qlik Sense administrator access to the QMC, and have authorization to add new nodes to the system. As the attacker adds a new node to the system, the XSS script would be placed as the name of the new node. The script would execute whenever an administrator with proper authorization navigates to the QMC page that lists the nodes in the system.

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