Directory Traversal Issue in QlikView Server

Qlik bug ID: QV-15634

Published: 2018-11-26

Updated: Initial Release

CVSS 3 Score 7.5

Executive Summary

A vulnerability has been identified in QlikView Server that allows a user with network access to the application the ability to download files stored on the server's file system.

Affected Software

All QlikView Server versions before 11.20 SR18, 12.00 SR6, 12.10 SR10 and November 2017 SR8 (12.20 SR8).

QlikView Server November 2018 (12.30) is unaffected.

Severity Rating

This vulnerability is rated as high due to the possibility of sensitive files from the hosting server being disclosed to unauthorized users.

The calculated CVSS score: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 7.5 (High)

Vulnerability Details

Due to insufficient sanitization of user input, a user can manipulate their Browser requests to request files from the hosting server that they should not have access to. This type of vulnerability is commonly known as a *Directory Traversal*.

Recommendation

Customers are recommended to upgrade their QlikView Server installs to at least 11.20 SR18, 12.00 SR6, 12.10 SR10, November 2017 SR8 (12.20 SR8). or November 2018 (12.30).

Acknowledgement

Qlik would like to thank Linfosys B.V. (https://www.linfosys.nl/) for responsibly disclosing this issue to us.