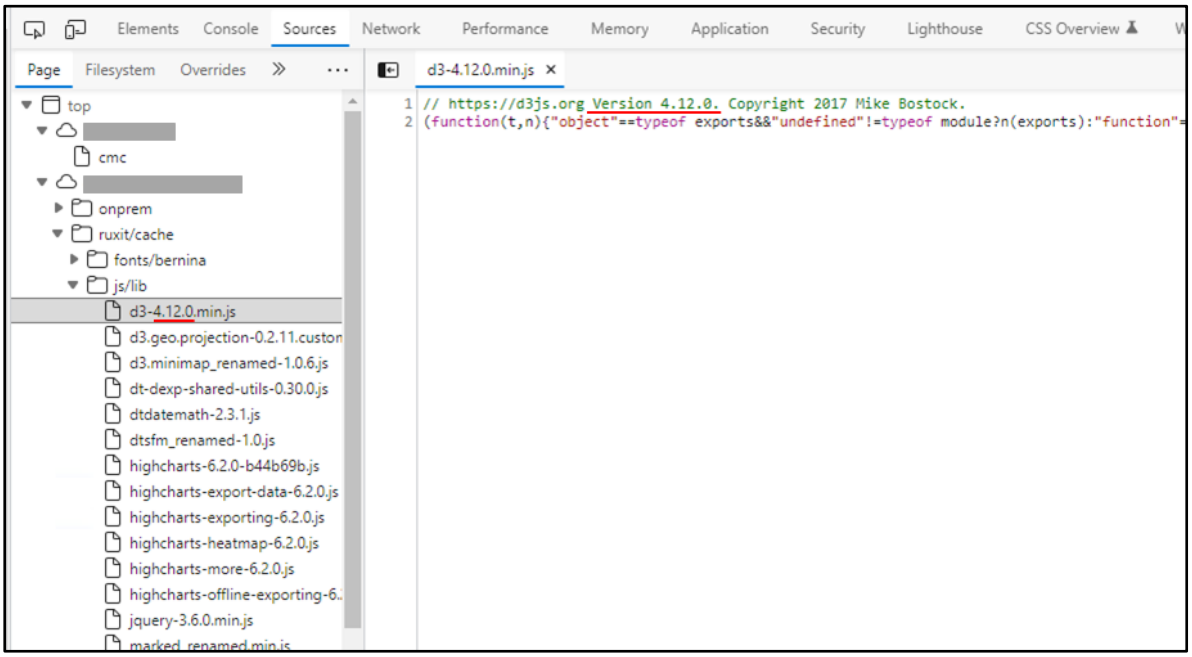
Title: Dynatrace should be configured to prevent disclosure of web component and configuration information in the body web pages

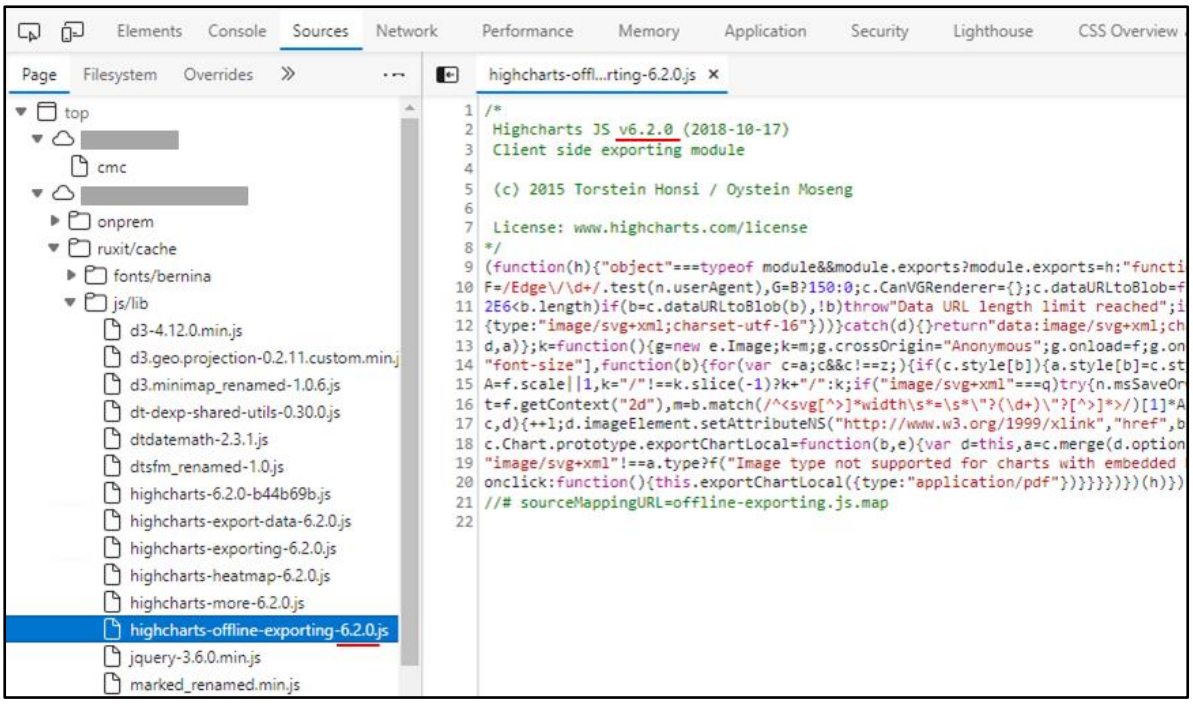
It was noted that versions of web components were revealed in the source code files of the Dynatrace application.

The following list details the source code files where versions of web components were revealed:

- jQuery 3.2.0
  - /ruxit/cache/js/lib/jquery-3.2.0.min.js
- d3 Version 4.12.0
  - /ruxit/cache/js/lib/d3-4.12.0.min.js
- Highcharts JS v6.2.0 (2018-10-17)
  - /ruxit/cache/js/lib/highcharts-6.2.0.js
  - /ruxit/cache/js/lib/highcharts-export-data-6.2.0.js
  - /ruxit/cache/js/lib/highcharts-exporting-6.2.0.js
  - /ruxit/cache/js/lib/highcharts-heatmap-6.2.0.js
  - /ruxit/cache/js/lib/highcharts-more-6.2.0.js
  - /ruxit/cache/js/lib/highcharts-offline-exporting-6.2.0.js
- topojson Version 2.2.0
  - /ruxit/cache/js/lib/topojson-2.2.0.min.js



Version of d3 is revealed to be 4.12.0 in the source code.



Version of Highcharts is revealed to be 6.2.o in the source code.

Implications

The exposure of configuration information provides an attacker information regarding the server. This information may allow an attacker to work with when crafting exploits for the system and increases the risk of the system being compromised.

Allowing unnecessary information disclosure relating to web component versions can allow an attacker to identify specific vulnerabilities or exploits for the system and increase the risk of the system being compromised.