**Includes front-end JavaScript libraries with known security vulnerabilities**

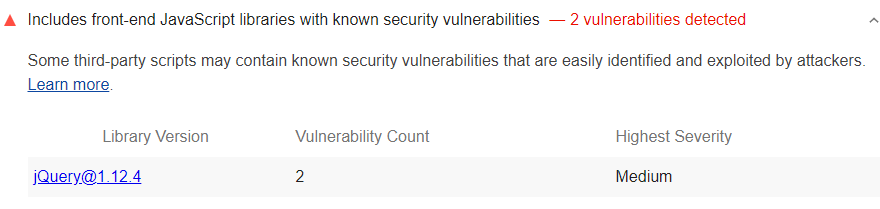
May 2, 2019 • Updated Jun 4, 2020

Appears in: [Best Practices audits](https://web.dev/lighthouse-best-practices)

Intruders have automated web crawlers that can scan your site for known security vulnerabilities. When the web crawler detects a vulnerability, it alerts the intruder. From there, the intruder just needs to figure out how to exploit the vulnerability on your site.

**How this Lighthouse audit fails** [**#**](https://web.dev/no-vulnerable-libraries/?utm_source=lighthouse&utm_medium=devtools#how-this-lighthouse-audit-fails)

[Lighthouse](https://developers.google.com/web/tools/lighthouse/) flags front-end JavaScript libraries with known security vulnerabilities:



To detect vulnerable libraries, Lighthouse:

* Runs [Library Detector For Chrome](https://www.npmjs.com/package/js-library-detector).
* Checks the list of detected libraries against [snyk's Vulnerability DB](https://snyk.io/vuln?packageManager=all).

Each Best Practices audit is weighted equally in the Lighthouse Best Practices Score. Learn more in [The Best Practices score](https://developers.google.com/web/tools/lighthouse/v3/scoring#best-practices).

**Stop using insecure JavaScript libraries** [**#**](https://web.dev/no-vulnerable-libraries/?utm_source=lighthouse&utm_medium=devtools#stop-using-insecure-javascript-libraries)

Stop using each of the libraries that Lighthouse flags. If the library has released a newer version that fixes the vulnerability, upgrade to that version. If the library hasn't released a new version or is no longer maintained, consider using a different library.