Server-side Request Forgery (SSRF)

Affecting phantomjs-seo package, versions *

INTRODUCED: 3 SEP 2020 CVE-2020-7739 CWE-918 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `phantomjs-seo`.

Overview

phantomjs-seo is an express middleware for prerendering pages with phantomjs for search engine crawling

Affected versions of this package are vulnerable to Server-side Request Forgery (SSRF). It is possible for an attacker to craft a `url` that will be passed to a `PhantomJS` instance allowing for an SSRF attack.

PoC

```
mkdir poc cd poc npm init -y npm install express npm install phantomjs-seo
```

create `index.js` with basic Express app

```
const express = require('express') const app = express() const port = 3000 // phantomjs-seo middleware
init const seo = require('phantomjs-seo') app.use(seo)

app.get('/', (req, res) => res.send('Hello World!')) app.listen(port, () => console.log(Example app
listening at http://localhost:${port}))
```

run it:

```
node index.js
```

References

- GitHub Vulnerable Code

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH

See more

NVD 8.2 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk Learn

Learn about Server-side Request Forgery (SSRF) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-PHANTOMJSSEO-609638
Published	5 Oct 2020
Disclosed	3 Sep 2020
Credit	Vasilii Ermilov

Report a new vulnerability | Found a mistake?