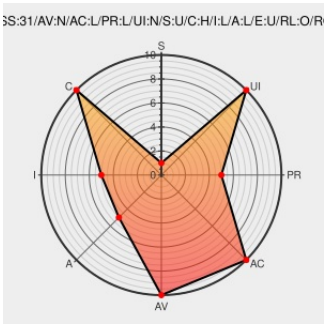
CVE-2020-7749

Published on: 10/20/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-7749

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Osm-static-maps from Osm-static-maps Project contain the following vulnerability:

This affects all versions of package osm-static-maps. 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.

CVE-2020-7749 has been assigned by report@snyk.io to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	LOW	LOW

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Server-side Request Forgery (SSRF) in osm-static-maps | Snyk	Exploit, Third Party Advisory	MISC snyk.io/vuln/SNYK-JS-OSMSTATICMAPS-609637

	snyk.io text/html	
fix: escape special characters before insertion to template by snoopysecurity · Pull Request #24 · jperelli/osm-static-maps · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/jperelli/osm-static-maps/pull/24
osm-static-maps/template.html at master · jperelli/osm-static-maps · GitHub	Broken Link github.com text/html	MISC github.com/jperelli/osm-static-maps/blob/master/src/template.html%23L142

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

981834 Nodejs (npm) Security Update for osm-static-maps (GHSA-pxcf-v868-m492)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Osm-static-maps Project	Osm-static-maps	All	All	All	All
Application	Osm-static-maps Project	Osm-static-maps	All	All	All	All

cpe:2.3:a:osm-static-maps_project:osm-static-maps:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:osm-static-maps_project:osm-static-maps:*:*:*:*:*:node.js:*:*:

Discovery Credit

Vasilii Ermilov

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report