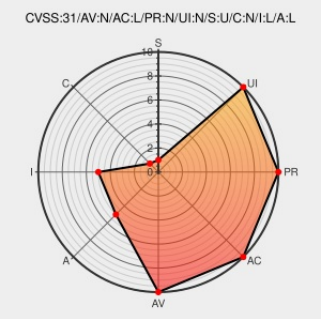
CVE-2023-5654

Published on: Not Yet Published

Last Modified on: 10/27/2023 09:53:00 PM UTC

CVE-2023-5654

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



Certain versions of React-devtools from Facebook contain the following vulnerability:

The React Developer Tools extension registers a message listener with window.addEventListener('message', <listener>) in a content script that is accessible to any webpage that is active in the browser. Within the listener is code that requests a URL derived from the received message via fetch(). The URL is not validated or sanitised before it is fetched, thus allowing a malicious web page to arbitrarily fetch URL's via the victim's browser.

CVE-2023-5654 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Meta** - **React Developer Tools Extension** version **= < 4.28.4**

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
React Developer Tools v4.27.8 Arbitrary URL Fetch via Malicious Web Page · GitHub	gist.github.com text/html	MISC gist.github.com/CalumHutton/1fb89b64409570a43f89d1fd3274b231

Related QID Numbers

995679 NodeJs (Npm) Security Update for react-devtools-core (GHSA-rxrc-rgv4-jpvx)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Facebook	React-devtools	All	All	All	All

cpe:2.3:a:facebook:react-devtools:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→