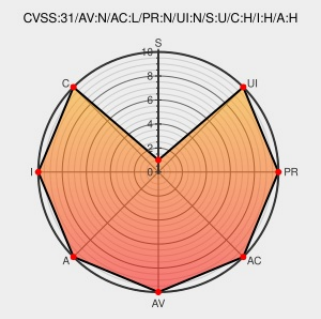
CVE-2020-7623

Published on: 04/02/2020 12:00:00 AM UTC

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

CVE-2020-7623

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



Certain versions of Jscover from Jscover Project contain the following vulnerability:

jscover through 1.0.0 is vulnerable to Command Injection. It allows execution of arbitrary command via the source argument.

CVE-2020-7623 has been assigned by report@snyk.io to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
jscover/jscover.js at master · node-modules/jscover · GitHub	Exploit, Third Party Advisory, github.com, text/html	MISC github.com/node-modules/jscover/blob/master/lib/jscover.js#L59,

Command Injection in jscover | Snyk

Third Party Advisory
snyk.io
text/html

MISC snyk.io/vuln/SNYK-JS-JSCOVER-564250

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jscover Project	Jscover	All	All	All	All

cpe:2.3:a:jscover_project:jscover:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→