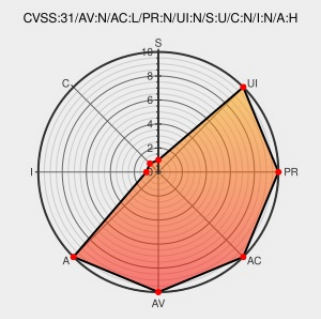
CVE-2022-22143

Published on: Not Yet Published

Last Modified on: 05/11/2022 05:45:00 PM UTC

CVE-2022-22143

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



Certain versions of Convict from Mozilla contain the following vulnerability:

The package convict before 6.2.2 are vulnerable to Prototype Pollution via the convict function due to missing validation of parentKey. **Note:** This vulnerability derives from an incomplete fix of another [vulnerability](https://security.snyk.io/vuln/SNYK-JS-CONVICT-1062508)

CVE-2022-22143 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
Prototype Pollution in convict | CVE-2022-22143 | Snyk	snyk.io, text/html	MISC snyk.io/vuln/SNYK-JS-CONVICT-2340604
More complete fix against prototype pollution -	github.com	MISC github.com/mozilla/node-convict/commit/3b86be087d8f14681a9c88

More complete fix against prototype pollution mozilla/node-convict@3b86be0 · GitHub	github.com text/html	MISC github.com/mozilla/node-convict/commit/3b86be0...
node-convict/main.js at 5eb1314f85346760a3c31cb14510f2f0af11d0d3 · mozilla/node-convict · GitHub	github.com text/html	MISC github.com/mozilla/node-convict/blob/5eb1314f85346760a3c31cb14510f2f0af11d0d3/packages/convic

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Convict	All	All	All	All

cpe:2.3:a:mozilla:convict:*:*:*:*:*:node.js:*:*:

Discovery Credit

P.Adithya Srinivas

Masudul Hasan Masud Bhuiyan

Cristian-Alexandru Staicu

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-22143 : The package convict before 6.2.2 are vulnerable to Prototype Pollution via the convict function du… twitter.com/i/web/status/1…	2022-05-01 15:38:51
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-22143 The package convict before 6.2.2 are vulnerable to Prototype Poll… twitter.com/i/web/status/1…	2022-05-01 16:55:59
/r/netcve	CVE-2022-22143	2022-05-01 17:29:21

← Previous ID

Next ID→