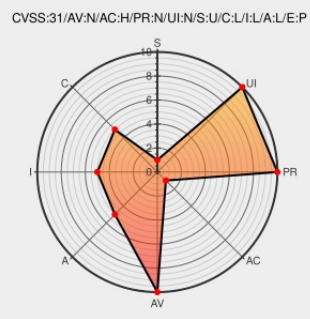
CVE-2021-23380

Published on: 04/18/2021 12:00:00 AM UTC

Last Modified on: 06/28/2022 02:11:00 PM UTC

CVE-2021-23380

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



Certain versions of Roar-pidusage from Roar-pidusage Project contain the following vulnerability:

This affects all versions of package roar-pidusage. If attacker-controlled user input is given to the stat function of this package on certain operating systems, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.

CVE-2021-23380 has been assigned by report@snyk.io to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.3 - HIGH

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

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
Arbitrary Command Injection in roar-pidusage | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-ROARPIDUSAGE-1078528
pidusage/stats.js at	github.com	MISC

pidusage/stats.js at 772cd2bd675ff7b1244b6fe3d7541692b1b9e42c · Svjard/pidusage · GitHub

github.com text/html

github.com/Svjard/pidusage/blob/772cd2bd675ff7b1244b6fe3d7541692b1b9

Related QID Numbers

982676 Nodejs (npm) Security Update for roar-pidusage (GHSA-xfxf-qw26-hr33)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Roar-pidusage Project	Roar-pidusage	All	All	All	All

cpe:2.3:a:roar-pidusage_project:roar-pidusage:*:*:*:*:*:node.js:*:*:

Discovery Credit

OmniTaint

← Previous ID

Next ID→