



# CVE-2020-28469

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-28469
<b>State</b>	PUBLIC
<b>Assigner</b>	report@snyk.io
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-03 16:15:00 UTC
<b>Updated</b>	2022-03-29 16:39:00 UTC
<b>Description</b>	This affects the package glob-parent before 5.1.2. The enclosure regex used to check for strings ending in enclosure conta

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Gulpjs</a>	<a href="#">Glob-parent</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Cloud Native Core Policy</a>	1.14.0	All	All	All

## References

Reference	Source	Link	Tags
Regular Expression Denial of Service (ReDoS) in org.webjars.bowergithub.es128:glob-parent   Snyk	MISC	<a href="#">snyk.io</a>	
Regular Expression Denial of Service (ReDoS) in org.webjars.npm:glob-parent   Snyk	MISC	<a href="#">snyk.io</a>	
<a href="#">github.com/gulpjs/glob-parent/blob/6ce8d11f2f1ed8e80a9526b1dc8cf3aa71f43...</a>	MISC	<a href="#">github.com</a>	
Oracle Critical Patch Update Advisory - January 2022	MISC	<a href="#">www.oracle.com</a>	
Release v5.1.2 · gulpjs/glob-parent · GitHub	MISC	<a href="#">github.com</a>	
fix: eliminate ReDoS by Trott · Pull Request #36 · gulpjs/glob-parent · GitHub	MISC	<a href="#">github.com</a>	
Regular Expression Denial of Service (ReDoS) in glob-parent   Snyk	MISC	<a href="#">snyk.io</a>	
<a href="#">glob-parent/index.js at 6ce8d11f2f1ed8e80a9526b1dc8cf3aa71f43474 · gulpjs/glob-parent · GitHub</a>	MITRE	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canon
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canon

## Vendor Comments And Credit

## Legacy QID Mappings

159554 Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2021-5171)
159622 Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2022-0350)
160111 Oracle Enterprise Linux Security Update for nodejs and nodejs-nodemon (ELSA-2022-6595)
239590 Red Hat Update for rh-nodejs12-nodejs and rh-nodejs12-nodejs-nodemon (RHSA-2021:3281)
239591 Red Hat Update for rh-nodejs14-nodejs and rh-nodejs14-nodejs-nodemon (RHSA-2021:3280)
239970 Red Hat Update for nodejs:16 security (RHSA-2021:5171)
240037 Red Hat Update for nodejs:14 security (RHSA-2022:0246)
240051 Red Hat Update for nodejs:14 security (RHSA-2022:0350)
240676 Red Hat Update for nodejs and nodejs-nodemon (RHSA-2022:6595)
377422 Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2022:0014)
378599 Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)
378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
940355 AlmaLinux Security Update for nodejs:16 (ALSA-2021:5171)
940448 AlmaLinux Security Update for nodejs:14 (ALSA-2022:0350)
940678 AlmaLinux Security Update for nodejs and nodejs-nodemon (ALSA-2022:6595)
960322 Rocky Linux Security Update for nodejs:16 (RLSA-2021:5171)
960531 Rocky Linux Security Update for nodejs and nodejs-nodemon (RLSA-2022:6595)
960863 Rocky Linux Security Update for nodejs:14 (RLSA-2022:0350)
982275 Nodejs (npm) Security Update for glob-parent (GHSA-ww39-953v-wcq6)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)