



CVE-2020-7661

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

Summary

CVE	CVE-2020-7661
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-04 18:15:00 UTC
Updated	2020-06-10 15:26:00 UTC
Description	all versions of url-regex are vulnerable to Regular Expression Denial of Service. An attacker providing a very long string in S

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Url-regex Project	Url-regex	All	All	All	All
Application	Url-regex Project	Url-regex	All	All	All	All

References

Reference
[VULNERABILITY] Parsing a long String will result in 100% CPU usage and `String.test` will never finish · Issue #70 · kevva/url-regex · GitHub
Regular Expression Denial of Service (ReDoS) in url-regex Snyk
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980768](#) Nodejs (npm) Security Update for url-regex (GHSA-v4rh-8p82-6h5w)

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report