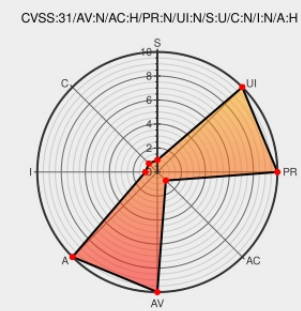
CVE-2021-43307

Published on: Not Yet Published

Last Modified on: 07/18/2023 01:53:00 PM UTC

CVE-2021-43307 - advisory for

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



Certain versions of Semver-regex from Semver-regex Project contain the following vulnerability:

An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the semver-regex npm package, when an attacker is able to supply arbitrary input to the test() method

CVE-2021-43307 has been assigned by security@jfrog.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **semver-regex** - **semver-regex** version **< 3.1.4**

Affected Vendor/Software: **semver-regex** - **semver-regex** version **< 4.0.3**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link

semver-regex ReDoS | XRAY-211349 - JFrog Security Research	research.jfrog.com text/html	MISC research.jfrog.com/vulnerabilities/semver-regex-redos-xray-211349/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:semver-regex_project:semver-regex:*:*:*:*:*:*:*:*:

Discovery Credit

Denys Vozniuk from JFrog Security Research

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	cve.report/CVE-2021-43307 An exponential ReDoS Regular Expression Denial of Service can be triggered in the semver… twitter.com/i/web/status/1…	2022-06-02 16:27:44

← Previous ID

Next ID→