



CVE-2021-43309

Published on: Not Yet Published

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

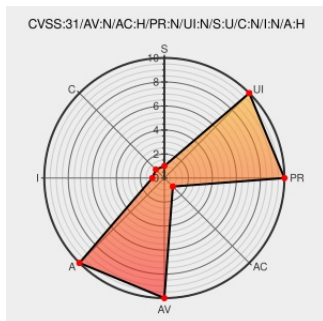
CVE-2021-43309

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Uri-template-lite](#) from [Litejs](#) contain the following vulnerability:

An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the uri-template-lite npm package, when an attacker is able to supply arbitrary input to the "URI.expand" method

CVE-2021-43309 has been assigned by security@jfrog.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **uri-template-lite** - **uri-template-lite** version >=

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

CVE References

Description	Tags	Link
uri-template-lite URI.expand ReDoS XRAY-211351 - JFrog Security Research	research.jfrog.com text/html	MISC research.jfrog.com/vulnerabilities/uri-template-lite-redos-xray-211351/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Feedback/Report from GitHub

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Litejs	Uri-template-lite	All	All	All	All
cpe:2.3:a:litejs:uri-template-lite:*:*:*:*:node.js:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-43309 : An exponential ReDoS Regular Expression Denial of Service can be triggered in the uri-template-l... twitter.com/i/web/status/1...	2022-08-24 16:14:37
 @LinInfoSec	Npm - CVE-2021-43309: research.jfrog.com/vulnerabilitie...	2022-08-24 19:00:38
 @threatmeter	CVE-2021-43309 An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the uri-template-lit... twitter.com/i/web/status/1...	2022-08-24 23:07:55
 @ColorTokensInc	Emerging Vulnerability Found CVE-2021-43309 - An exponential ReDoS (Regular Expression Denial of Service) can be tr... twitter.com/i/web/status/1...	2022-08-24 23:08:04
 @threatmeter	CVE-2021-43309 An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the uri-template-lit... twitter.com/i/web/status/1...	2022-08-25 07:09:40
 @Har_sia	CVE-2021-43309 har-sia.info/CVE-2021-43309... #HarsialInfo	2022-08-26 07:01:10
 /r/netcve	CVE-2021-43309	2022-08-24 17:39:02

[← Previous ID](#)[Next ID →](#)

© CVE.report 2023   |

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](#)