



CVE-2020-7761

Published on: 11/05/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:53 PM UTC

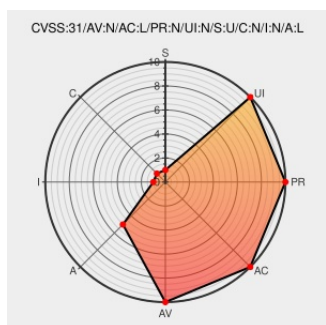
CVE-2020-7761

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Kafe](#) from [Absolunet](#) contain the following vulnerability:

This affects the package `@absolunet/kafe` before 3.2.10. It allows cause a denial of service when validating crafted invalid emails.

CVE-2020-7761 has been assigned by report@snyk.io to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

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
Switch email pattern to practical implementation of RFC 5322 · absolunet/kafe@c644c79 · GitHub	Broken Link github.com text/html	MISC github.com/absolunet/kafe/commit/c644c798bfcdd1b0bbb1f0ca59e2e2664ff3fdd0%23diff-f0f4b5b19ad46588ae9d7dc1889f681252b0698a4ead3a77b7c7d127ee657857

MISC snyk.io/vuln/SNYK-JS-ABSOLUNETKAFE-1017403

Related QID Numbers

Known Affected Configurations (CPE V2.3)

Discovery Credit

Yeting Li

Next ID→

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