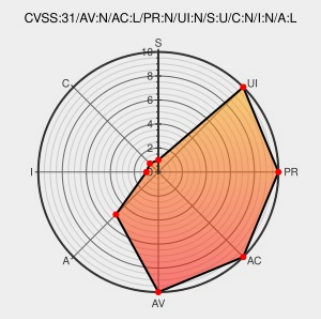
CVE-2020-7761

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/c644c798bfcdc1b0bbb1f0ca59e2e2664ff3fdd0%23diff-f0f4b5b19ad46588ae9d7dc1889f681252b0698a4ead3a77b7c7d127ee657857

Regular Expression Denial of Service (ReDoS) in @absolunet/kafe | Snyk	Broken Link snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-ABSOLUNETKAFE-1017403

Related QID Numbers

982610 Nodejs (npm) Security Update for @absolunet/kafe (GHSA-hgpf-97c5-74fc)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Absolunet	Kafe	All	All	All	All
Application	Absolunet	Kafe	All	All	All	All

cpe:2.3:a:absolunet:kafe:*:*:*:*:*:*:*:*:

cpe:2.3:a:absolunet:kafe:*:*:*:*:*:*:*:*:

Discovery Credit

Yeting Li

← Previous ID

Next ID→