



CVE-2026-3455

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

Summary

CVE	CVE-2026-3455
State	PUBLISHED
Assigner	snyk
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-03 05:17:25 UTC
Updated	2026-04-29 01:00:01 UTC
Description	Versions of the package mailparser before 3.9.3 are vulnerable to Cross-site Scripting (XSS) via the textToHtml() function c

Risk And Classification

Primary CVSS: v4.0 2 LOW from report@snyk.io

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-79 | CWE-79 Cross-site Scripting (XSS)

Version	Source	Type	Score	Severity	Vector
4.0	report@snyk.io	Secondary	2	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:P/C...
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:P
3.1	report@snyk.io	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N/E:P

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nodemailer	Mailparser	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Mailparser	affected 3.9.3 semver	Not specified

References

Reference	Source	Link	Tags
github.com/nodemailer/mailparser/issues/412	report@snyk.io	github.com	Issue Tracking
github.com/nodemailer/mailparser/commit/921a67df4cfb38f0b411037d7b26fd4...	report@snyk.io	github.com	Patch
gist.github.com/hayageek/7fcb225e3b1ea9a341d560403fbb585a	report@snyk.io	gist.github.com	Exploit, Third Party A
security.snyk.io/vuln/SNYK-JS-MAILPARSER-15204032	report@snyk.io	security.snyk.io	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Ravishanker Kusuma (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

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