



CVE-2021-23400

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

Summary

CVE	CVE-2021-23400
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-29 12:15:00 UTC
Updated	2021-07-06 18:48:00 UTC
Description	The package nodemailer before 6.6.1 are vulnerable to HTTP Header Injection if unsanitized user input that may contain ne

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
v6.6.1 · nodemailer/nodemailer@7e02648 · GitHub	MISC	github.com	
Header injection vulnerability in address object · Issue #1289 · nodemailer/nodemailer · GitHub	MISC	github.com	
HTTP Header Injection in org.webjars.npm:nodemailer Snyk	MISC	snyk.io	
HTTP Header Injection in nodemailer Snyk	MISC	snyk.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

Vendor Comments And Credit

Discovery Credit

LEGACY: Adam Williams

Legacy QID Mappings

[179423](#) Debian Security Update for node-nodemailer (CVE-2021-23400)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)