



CVE-2021-43854

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-43854
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-23 18:15:00 UTC
Updated	2022-01-04 16:38:00 UTC
Description	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting research an

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Resolved serious ReDoS in PunktSentenceTokenizer by tomaarsen · Pull Request #2869 · nltk/nltk · GitHub	MISC	github.com
word_tokenize/EN hangs on incorrect strings · Issue #2866 · nltk/nltk · GitHub	MISC	github.com
Inefficient Regular Expression Complexity in nltk (word_tokenize, sent_tokenize) · Advisory · nltk/nltk · GitHub	CONFIRM	github.com
Resolved serious ReDoS in PunktSentenceTokenizer (#2869) · nltk/nltk@1405aad · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184262 Debian Security Update for nltk (CVE-2021-43854)

© [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](#)