



# Arbitrary Code Execution in NLTK StanfordSegmenter via Untrusted JAR Loading

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

## Summary

<b>CVE</b>	CVE-2026-0848
<b>State</b>	PUBLISHED
<b>Assigner</b>	@huntr_ai
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-05 21:16:14 UTC
<b>Updated</b>	2026-04-21 14:56:46 UTC
<b>Description</b>	NLTK versions <=3.9.2 are vulnerable to arbitrary code execution due to improper input validation in the StanfordSegmenter

## Risk And Classification

**Primary CVSS:** v3.0 10 CRITICAL from security@huntr.dev

**CVSS:** 3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**EPSS:** 0.002900000 probability, percentile 0.524890000 (date 2026-04-22)

**Problem Types:** CWE-20 | NVD-CWE-noinfo | CWE-20 CWE-20 Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.0	security@huntr.dev	Secondary	10	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.0	CNA	DECLARED	10	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nltk	Nltk/nltk	affected unspecified latest custom	Not specified

### References

Reference	Source	Link	Tags
huntr.com/bounties/08b109bb-ac24-403f-9422-1c246ce60202	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://huntr.com">huntr.com</a>	Exploit, Vendor A
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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

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

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)