



Apache OpenNLP: Arbitrary Class Instantiation via Model Manifest in ExtensionLoader

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

Summary

CVE	CVE-2026-42027
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 17:16:24 UTC
Updated	2026-05-05 19:32:23 UTC
Description	Arbitrary Class Instantiation via Model Manifest in Apache OpenNLP ExtensionLoader Versions Affected: before 2.5.9, before

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from ADP

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

EPSS: 0.002860000 probability, percentile 0.519510000 (date 2026-05-05)

Problem Types: CWE-470 | CWE-470 CWE-470 Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache OpenNLP	affected 2.5.9 semver	Not specified
CNA	Apache Software Foundation	Apache OpenNLP	affected 3.0 3.0.0-M3 semver	Not specified

References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/05/01/20	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
lists.apache.org/thread/ltlo4powjfc0w2w2yy1o5tc7q1gcb2y	security@apache.org	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

Vendor Comments And Credit

Discovery Credit

CNA: Subramanian S (en)

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](#) 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