Improper Restriction of XML External Entity Reference in stanfordnlp/corenlp

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-0239
State	PUBLISHED
Assigner	@huntrdev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-17 07:15:06 UTC
Updated	2026-04-16 16:07:03 UTC
Description	corenlp is vulnerable to Improper Restriction of XML External Entity Reference

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.000420000 probability, percentile 0.127580000 (date 2026-04-21)

Problem Types: CWE-611 | CWE-611 CWE-611 Improper Restriction of XML External Entity Reference

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.0	security@huntr.dev	Secondary	4.7	MEDIUM	CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N
3.0	CNA	DECLARED	4.7	MEDIUM	CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Stanford	Corenlp	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Stanfordnlp	Stanfordnlp/corenlp	affected unspecified 4.3.3 custom	Not specified
ADP	Stanford	Corenlp	affected 4.3.3 custom	Not specified

References

Reference	Source	Link	Tags
huntr – the Bug Bounty Platform for any GitHub repository	af854a3a-2127-422b-91ae-364da2661108	huntr.dev	Exploit
Fix XML schema vulnerability · stanfordnlp/CoreNLP@1940ffb · GitHub	af854a3a-2127-422b-91ae-364da2661108	github.com	Patch,
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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