



# Joomla! Core - [20260303] - XSS vector in com\_associations comparison view

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

## Summary

<b>CVE</b>	CVE-2026-21631
<b>State</b>	PUBLISHED
<b>Assigner</b>	Joomla
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-01 10:16:16 UTC
<b>Updated</b>	2026-04-09 19:55:58 UTC
<b>Description</b>	Lack of output escaping leads to a XSS vector in the multilingual associations component.

## Risk And Classification

**Primary CVSS:** v4.0 5.9 MEDIUM from security@joomla.org

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000180000 probability, percentile 0.046820000 (date 2026-04-07)

**Problem Types:** CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	security@joomla.org	Secondary	5.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:U
4.0	CNA	CVSS	5.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:U
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/L/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joomla	Joomla!	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

CNA	Joomla! Project	Joomla! CMS	affected 4.0.0-5.4.3	Not specified
CNA	Joomla! Project	Joomla! CMS	affected 6.0.0-6.0.3	Not specified

## References

Reference	Source	Link	Tag
github.com/Shirshaw64p/security-advisories/tree/main/CVE-2026-21631	security@joomla.org	<a href="https://github.com">github.com</a>	Explo
developer.joomla.org/security-centre/1029-20260303-core-xss-vector-in-com-associat...	security@joomla.org	<a href="https://developer.joomla.org">developer.joomla.org</a>	Ven
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canc
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canc

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Shirsendu Mondal & Md Tanzimul Alam Fahim, UNC Pembroke (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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

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)