



XWiki Platform affected by remote code execution with script right through unprotected Velocity scripting API

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

Summary

CVE	CVE-2026-33229
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 16:16:23 UTC
Updated	2026-04-10 21:16:24 UTC
Description	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Prior to 17.4.8 and 17.1.0

Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/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: 0.000330000 probability, percentile 0.095450000 (date 2026-04-10)

Problem Types: CWE-862 | CWE-862 CWE-862: Missing Authorization

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/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
4.0	CNA	DECLARED	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/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
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 v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSG:X/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

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	Xwiki	Xwiki-platform	affected >= 17.0.0-rc-1, < 17.4.8	Not specified
CNA	Xwiki	Xwiki-platform	affected >= 17.5.0-rc-1, < 17.10.1	Not specified
CNA	Org.xwiki.platform	Xwiki-platform-legacy-oldcore	affected >= 17.0.0-rc-1, < 17.4.8	Not specified

CNA	Org.xwiki.platform	Xwiki-platform-legacy-oldcore	affected >= 17.5.0-rc-1, < 17.10.1	Not specified
CNA	Org.xwiki.platform	Xwiki-platform-oldcore	affected >= 17.0.0-rc-1, < 17.4.8	Not specified
CNA	Org.xwiki.platform	Xwiki-platform-oldcore	affected >= 17.5.0-rc-1, < 17.10.1	Not specified

References

Reference	Source	Link	Tags
jira.xwiki.org/browse/XWIKI-23702	security-advisories@github.com	jira.xwiki.org	
jira.xwiki.org/browse/XWIKI-23698	security-advisories@github.com	jira.xwiki.org	
github.com/xwiki/xwiki-platform/commit/9fe84da66184c05953df9466cf3a4acd1...	security-advisories@github.com	github.com	
github.com/xwiki/xwiki-platform/security/advisories/GHSA-h259-74h5-4rh9	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#) 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](#)