

CVE-2025-24893

XWiki Platform Eval Injection Vulnerability

Exigent

CISA KEV since Oct 30, 2025

Actively exploited

Public exploit module (Metasploit)

XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any guest can perform arbitrary remote code execution through a request to `SolrSearch`. This impacts the confidentiality, integrity and availability of the whole XWiki installation. To reproduce on an instance, without being logged in, go to

EVRS 90/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.96th percentile · FIRST	CISA DEADLINE Nov 20, 2025 CISA federal deadline · Overdue by 11 months
---	---	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEY	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

```
`<host>/xwiki/bin/get/Main/SolrSearch?
```

media=rss&text=%7D%7D%7D%7B%7Basync%20async%3Dfalse%7D%7D%7B%7Bgroovy%7D%7Dprintln%28"Hello%20from"%20%2B%20"%20search

If there is an output, and the title of the RSS feed contains `Hello from search text:42`, then the instance is vulnerable. This vulnerability has been patched in XWiki 15.10.11, 16.4.1 and 16.5.0RC1. Users are advised to upgrade. Users unable to upgrade may edit `Main.SolrSearchMacros` in `SolrSearchMacros.xml` on line 955 to match the `rawResponse` macro in `macros.vm#L2824` with a content type of `application/xml`. instead of simply outputting the content of the feed.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
xwiki	$\geq 5.4 < 15.10.11$ $\geq 16.0.0 < 16.4.1$ 5.3	15.10.11 · 16.4.1	NVD

Sources

Vendor guidance	github.com/xwiki/xwiki-platform/commit/67021db9b8ed26c2236a653269302a86bf01ef40	Additional guidance	github.com/xwiki/xwiki-platform/security/advisories/GHSA-rr6p-3pfg-562j
NVD	nvd.nist.gov/vuln/detail/CVE-2025-24893	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-4562	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-24893

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.