

CVE-2024-27199

JetBrains TeamCity Relative Path Traversal Vulnerability

CISA KEV since Apr 20, 2026

Actively exploited

Ransomware use known

In JetBrains TeamCity before 2023.11.4 path traversal allowing to perform limited admin actions was possible

EVRS 93/100 Immediate priority	CVSS V3.1 7.3 High · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE May 4, 2026 CISA federal deadline · Overdue by 6 months
--	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
teamcity	< 2023.11.4	2023.11.4	NVD

Sources

Vendor guidance blog.jetbrains.com	github.com/advisories/GHSA-m7gg-q7qj-3r2r blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now/	Additional guidance NVD	jetbrains.com/privacy-security/issues-fixed/nvd.nist.gov/vuln/detail/CVE-2024-27199
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-24438
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-27199		

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