

CVE-2026-63077

JetBrains TeamCity Deserialization of Untrusted Data Vulnerability

Exigent CISA KEV since Aug 5, 2026 Actively exploited Ransomware use known Public exploit module (Metasploit)

In JetBrains TeamCity before 2026.1.3, 2025.11.7 unauthenticated remote code execution was possible via the agent polling protocol

EVRS 95/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.896 99.79th percentile · FIRST	CISA DEADLINE Aug 8, 2026 CISA federal deadline · Overdue by 2 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 90 days
☒ EPSS	0.896 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 in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
teamcity	< 2025.11.7 ≥ 2026.1 < 2026.1.3	2025.11.7 · 2026.1.3	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-94gx-v738-fx9w	blog.jetbrains.com	blog.jetbrains.com/teamcity/2026/07/cve-2026-63077/
jetbrains.com	jetbrains.com/privacy-security/issues-fixed/	BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	NVD	nvd.nist.gov/vuln/detail/CVE-2026-63077
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-49369
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-63077		

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