

CVE-2023-42793

JetBrains TeamCity Authentication Bypass Vulnerability

Exigent

CISA KEV since Oct 4, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

In JetBrains TeamCity before 2023.05.4 authentication bypass leading to RCE on TeamCity Server was possible

EVRS 94 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE Oct 25, 2023 KEV since 2023 · listed over a year
--	---	--	---

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	On the CISA KEV catalog for over two years
☒ 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 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	< 2023.05.4	2023.05.4	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-w796-2gq9-7jm8	Additional guidance	blog.jetbrains.com/teamcity/2023/09/cve-2023-42793-vulnerability-post-mortem/
blog.jetbrains.com	blog.jetbrains.com/teamcity/2023/09/critical-security-issue-affecting-teamcity-on-premises-update-to-2023-05-4-now/	NVD	nvd.nist.gov/vuln/detail/CVE-2023-42793
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-47222
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-42793		

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