

CVE-2024-27198

JetBrains TeamCity Authentication Bypass Vulnerability

Exigent
CISA KEV since Mar 7, 2024
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

In JetBrains TeamCity before 2023.11.4 authentication bypass allowing to perform admin actions was possible

EVRS 94 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Mar 28, 2024 KEV since 2024 · 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	< 2023.11.4	2023.11.4	NVD

Sources

Vendor guidance github.com/advisories/GHSA-xh94-49wq-7h2h jetbrains.com jetbrains.com/help/teamcity/teamcity-2023-11-4-release-notes.html	Additional guidance blog.jetbrains.com jetbrains.com/privacy-security/issues-fixed/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/cisa.gov/known-exploited-vulnerabilities-catalog
NVD nvd.nist.gov/vuln/detail/CVE-2024-27198	CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-24437	Current data evulnable.com/vulnerability-management/cve/CVE-2024-27198

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