



# CVE-2024-27199

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2024-27199
<b>State</b>	PUBLISHED
<b>Assigner</b>	JetBrains
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-03-04 18:15:09 UTC
<b>Updated</b>	2026-04-21 12:48:17 UTC
<b>Description</b>	In JetBrains TeamCity before 2023.11.4 path traversal allowing to perform limited admin actions was possible

## Risk And Classification

**Primary CVSS:** v3.1 7.3 HIGH from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

**EPSS:** 0.824720000 probability, percentile 0.992320000 (date 2026-04-20)

**CISA KEV:** Listed on 2026-04-20; due 2026-05-04; ransomware use Unknown

**Problem Types:** CWE-23 | CWE-22 | CWE-23 CWE-23

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	cve@jetbrains.com	Secondary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

### CISA Known Exploited Vulnerability

<b>Vendor</b>	JetBrains
<b>Product</b>	TeamCity
<b>Name</b>	JetBrains TeamCity Relative Path Traversal Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://www.jetbrains.com/privacy-security/issues-fixed/">https://www.jetbrains.com/privacy-security/issues-fixed/</a> ; <a href="https://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/">https://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/</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2024-27199">https://nvd.nist.gov/vuln/detail/CVE-2024-27199</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jetbrains	Teamcity	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	JetBrains	TeamCity	affected 2023.11.4 semver	Not specified

### References

Reference	Source	Link
Fixed security issues	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.jetbrains.com/privacy-security/issues-fixed/">www.je</a>
github.com/Stuub/RCity-CVE-2024-27198/blob/main/RCity.py	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://github.com/Stuub/RCity-CVE-2024-27198/blob/main/RCity.py">github.</a>
www.darkreading.com/cyberattacks-data-breaches/jetbrains-teamcity-mass-exploitati...	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.darkreading.com/cyberattacks-data-breaches/jetbrains-teamcity-mass-exploitati...">www.d</a>
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="http://www.cisa.gov/known-exploited-vulnerabilities-catalog">www.c</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.c</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-27199">nvd.nis</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="http://www.cisa.gov/known-exploited-vulnerabilities-catalog">www.c</a>

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

Source	Time	Event
ADP	2026-04-20T00:00:00.000Z	CVE-2024-27199 added to CISA KEV

  

Legacy QID Mappings
<a href="#">150825</a> JetBrains TeamCity Authentication Bypass Vulnerability (CVE-2024-27199)
<a href="#">379449</a> JetBrains TeamCity Multiple Authentication Bypass Vulnerabilities (TW-86500, TW-86502)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)