



# JetBrains TeamCity Authentication Bypass Vulnerability

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

## Summary

<b>CVE</b>	CVE-2023-42793
<b>State</b>	PUBLIC
<b>Assigner</b>	security@jetbrains.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-19 17:15:00 UTC
<b>Updated</b>	2023-10-03 15:44:00 UTC
<b>Description</b>	In JetBrains TeamCity before 2023.05.4 authentication bypass leading to RCE on TeamCity Server was possible

## Risk And Classification

**EPSS:** 0.929130000 probability, percentile 0.997700000 (date 2026-04-01)

**CISA KEV:** Listed on 2023-10-04; due 2023-10-25; ransomware use Known

**Problem Types:** CWE-288

## CISA Known Exploited Vulnerability

<b>Vendor</b>	JetBrains
<b>Product</b>	TeamCity
<b>Name</b>	JetBrains TeamCity Authentication Bypass Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://blog.jetbrains.com/teamcity/2023/09/critical-security-issue-affecting-teamcity-on-premises-update-to-2023-05-4-now/">https://blog.jetbrains.com/teamcity/2023/09/critical-security-issue-affecting-teamcity-on-premises-update-to-2023-05-4-now/</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-42793">https://nvd.nist.gov/vuln/detail/CVE-2023-42793</a>

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Tags
JetBrains TeamCity Unauthenticated Remote Code Execution ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
CVE-2023-42793   AttackerKB	MISC	<a href="https://attackerkb.com">attackerkb.com</a>	
Critical Authentication Bypass in JetBrains TeamCity CI/CD Servers   Rapid7 Blog	MISC	<a href="https://www.rapid7.com">www.rapid7.com</a>	
CVE-2023-42793 Vulnerability in TeamCity: Post-Mortem   The TeamCity Blog	MISC	<a href="https://blog.jetbrains.com">blog.jetbrains.com</a>	

Recently Patched TeamCity Vulnerability Exploited to Hack Servers - SecurityWeek	MISC	<a href="http://www.securityweek.com">www.securityweek.com</a>	
Fixed security issues	MISC	<a href="http://www.jetbrains.com">www.jetbrains.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, ana
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="http://www.cisa.gov">www.cisa.gov</a>	kev

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[378885](#) JetBrains TeamCity Authentication Bypass Vulnerability

© [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](#).

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