CYBER ADVISORY

TLP:CLEAR

06 February 2024

JetBrains TeamCity On-Premises Vulnerability

CVE-2024-23917 | On-Premises | RCE | Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-23917. The vulnerability affects JetBrains all versions of TeamCity On-Premises from 2017.1 through 2023.11.2. [1] The remote code execution (RCE) vulnerability may enable an unauthenticated attacker with HTTP and/or HTTPS access to a TeamCity server to bypass authentication checks and gain administrative control of the server.[2,3]

The Cal-CSIC recommends immediately upgrading to TeamCity On-Premises version 2023.11.3 or make use of the automatic update option within TeamCity.

For further information on applying upgrades, please refer to JeatBrains TeamCity Support.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To

	help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] VulDB; "JetBrains TeamCity Prior 2023.11.3 Authentication Bypass;" https://vuldb.com/?id.253013; accessed 06 February 2024
[2] JetBrains; "Critical Security Issue Affecting TeamCity On-Premises (CVE-2024-23917) – Update to 2023.11.3 Now;" https://blog.jetbrains.com/teamcity/2024/02/critical-security-issue-affecting-teamcity-on-premises-cve-2024-23917/; accessed 06 February 2024
[3] Bleeping Computer; "JetBrains warns of new TeamCity auth bypass vulnerability;" https://www.bleepingcomputer.com/news/security/jetbrains-warns-of-new-teamcity-auth-bypass-vulnerability/; accessed 06 February 2024