CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
04 March 2024

JetBrains TeamCity On-Premises Vulnerabilities

CVE-2024-27198 | CVE-2024-2719 | RCE | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of critical vulnerabilities known as CVE-2024-27198 and CVE-2024-27199.[1] The vulnerabilities affect all TeamCity On-Premises versions through 2023.11.3.[2] CVE-2024-27198 is an authentication bypass vulnerability in the web component of TeamCity that arises from an alternative path issue. CVE-2024-27199 is an authentication bypass vulnerability in the web component of TeamCity that arises from a path traversal issue. [3] Exploitation of the vulnerabilities could allow an attacker to achieve complete compromise of a vulnerable TeamCity server, potentially via unauthenticated remote code of execution, (RCE).[4]

The Cal-CSIC recommends immediately upgrading to JetBrains TeamCity On-Premises version 2023.11.4 or applying the automatic update option within TeamCity.

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

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.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

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] Helpnet Security; “Critical vulnerabilities in TeamCity JetBrains fixed, release of technical details imminent, patch quickly! (CVE-2024-27198, CVE-2024-27199);” https://www.helpnetsecurity.com/2024/03/04/cve-2024-27198-cve-2024-27199/; accessed 04 March 2024

[2] TeamCity Blog; “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/; accessed 04 March 2024

[3] CVE Details; “Vulnerability Details: CVE-2024-27198;” https://www.cvedetails.com/cve/CVE-2024-27198/; accessed 04 March 2024

[4] Rapid 7; “CVE-2024-27198 and CVE-2024-27199: JetBrains TeamCity Multiple Authentication Bypass Vulnerabilities (FIXED);” https://www.rapid7.com/blog/post/2024/03/04/etr-cve-2024-27198-and-cve-2024-27199-jetbrains-teamcity-multiple-authentication-bypass-vulnerabilities-fixed/?utm_campaign=sm-blog&utm_source=linkedin,twitter&utm_medium=organic-social; accessed 04 March 2024

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.