NCSC
National Cyber Security Centre

2403050151-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Security Issues Affecting JetBrains TeamCity On-Premises: CVE-2024-27198, CVE-2024-27199

Tuesday 5th March, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

JetBrains has released an update for on-premise versions of TeamCity. The update addresses two vulnerabilities:

- **CVE-2024-27198** has a CVE 3.0 score of 9.8 (Critical). This is a vulnerability in the web component of TeamCity that arises from an alternative path issue, allowing for authentication bypass.
- **CVE-2024-27199** has a CVE 3.0 score of 7.3 (High). This is a vulnerability in the web component of TeamCity that arises from an path traversal issue, allowing for authentication bypass.

The vulnerability was discovered by Rapid7, who have since released full details of the vulnerabilities.

Products Affected

All TeamCity On-Premises versions through to 2023.11.3.

Impact

- Exploitation of **CVE-2024-27198** may result in the attacker obtaining full control of a vulnerable TeamCity server.
- Exploitation of **CVE-2024-27199** may allow an attacker to reach a number of limited systems without authentication, modify settings on the system, as well as disclose sensitive information.

The vulnerabilities are not listed within the CISA Known Exploited Vulnerabilities (KEV) database.

Recommendations

The NCSC strongly advises affected organisations to upgrade their TeamCity systems as applicable.

Further information and some steps that organisations can take can be found here:

- 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://www.rapid7.com/blog/post/2024/03/04/etr-cve-2024-27198-and-cve-2024-27199-jetbrains-teamcity-multiple-authentication-bypass-vulnerabilities-fixed/

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie