GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

6 August 2026

Advisory 183: JetBrains TeamCity Deserialization of Untrusted Data Vulnerability (CVE-2026-63077)

Release Date: 5th August 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

JetBrains TeamCity is a continuous integration and delivery (CI/CD) server used to build, test and deploy software automatically. The sectors in Vanuatu most likely to operate one are:

- **Software development and ICT service companies**
- **Financial institutions, telecommunications operators and Internet Service Providers with in-house development teams**
- **Government agencies and their software contractors, including teams maintaining online services**

Organisations that do not operate TeamCity themselves may still be exposed through suppliers, as a contractor's build infrastructure forms part of your supply chain.

CERTVU advises organisations in these sectors to confirm, with their IT teams and any external developer, whether TeamCity is in use and has been patched.

What is it?

A Deserialization of Untrusted Data vulnerability (CWE-502, CVSS v3.1 9.8 Critical) in JetBrains TeamCity On-Premises. A remote, unauthenticated attacker with HTTP or HTTPS access can bypass authentication and execute arbitrary operating system commands with the privileges of the TeamCity server process. No credentials or user interaction are required.

The flaw is in the agent polling protocol used by build agents. An attacker sends a crafted payload to the polling endpoint, which the server deserializes and executes.

JetBrains disclosed the issue on 27 July 2026. On 5 August 2026 CISA added CVE-2026-63077 to its Known Exploited Vulnerabilities (KEV) catalogue, confirming exploitation in the wild, with a due date of 8 August 2026. CERTVU is not aware of verified public exploit code; this does not reduce the urgency.

What are the systems affected?

1. TeamCity On-Premises 2026.x before 2026.1.3 - Solution: upgrade to 2026.1.3 or above
2. TeamCity On-Premises 2025.11.x before 2025.11.7 - Solution: upgrade to 2025.11.7 or above
3. All earlier On-Premises versions are affected. TeamCity Cloud requires no action.
4. Where immediate upgrade is not possible, JetBrains provides a security patch plugin for 2017.1 and later. It is an interim measure, not a remediation.

What does this mean?

A CI/CD server holds the credentials and keys used to reach code repositories, artefact stores and deployment targets, and is trusted by every system it deploys to. JetBrains warns that exploitation exposes build environments, stored credentials and software supply chains: where a build server is compromised, every artefact it produced must be treated as suspect and every credential it held as disclosed.

CERTVU also notes a common misconception: because the build agent initiates the connection, administrators often assume the polling protocol is reachable only by trusted agents. It is not, so these servers are often more exposed than operators believe.

Mitigation process

CERTVU recommends;

1. Confirm whether TeamCity is present**:** Check with internal IT teams, including any instance deployed outside central IT, and with external software contractors.
2. Upgrade immediately: Upgrade to 2026.1.3 or 2025.11.7.
3. Restrict network access: Remove TeamCity servers from direct internet exposure, limit access to trusted internal networks and registered build agents, and place remote developer access behind a VPN.
4. Report: Report suspected compromise to CERTVU at incident@cert.gov.vu or (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-63077
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://blog.jetbrains.com/teamcity/2026/07/cve-2026-63077/