Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-63077: Critical TeamCity On-Premises RCE Under Active Exploitation

Date of Publication	Admiralty Code	TA Number
August 7, 2026	A1	TA2026226

Summary

First Seen: July 10, 2026
Publicly Disclosed: July 27, 2026
Affected Products: JetBrains TeamCity
Impact: CVE-2026-63077 is a critical (CVSS 9.8) deserialization of untrusted data flaw (CWE-502) in the JetBrains TeamCity On-Premises agent polling protocol that lets an unauthenticated attacker with HTTP(S) access bypass authentication and execute arbitrary OS commands with the server process's privileges, risking exposure of stored credentials and compromise of downstream CI/CD pipelines. All On-Premises versions are affected. Fixes are available in versions 2025.11.7 and 2026.1.3, with a security patch plugin for TeamCity 2017.1+, TeamCity Cloud is unaffected.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-63077	JetBrains TeamCity Deserialization of Untrusted Data Vulnerability	JetBrains TeamCity (On-Premises)	✗	✓	✓

Vulnerability Details

#1 CVE-2026-63077 is a critical unauthenticated remote code execution vulnerability in TeamCity On-Premises agent polling protocol. An unauthenticated remote attacker with HTTP(S) access to a TeamCity server can exploit the agent polling protocol to bypass authentication checks and execute arbitrary operating system commands with the privileges of the TeamCity server process. This vulnerability affects all TeamCity On-Premises versions.

#2 Because TeamCity orchestrates build pipelines, credential storage, and artifact production, the impact extends beyond a single host. A successful attack can expose TeamCity data, configurations, and stored credentials, modify server state, and potentially compromise the integrity of build artifacts and downstream CI/CD pipelines, placing the software supply chain at risk.

#3 The flaw was privately reported on July 10, 2026 under coordinated disclosure and publicly disclosed with a fix on July 27, 2026, so it was not a zero-day. JetBrains stated it was not aware of active exploitation at disclosure; on August 5, CISA added CVE-2026-63077 to its KEV catalog with an active-exploitation designation and an August 8, 2026 remediation deadline for federal agencies under BOD 26-04. The exploitation method, threat actor, and scale remain unknown, and no verified public PoC exists.

#4 The issue is fixed in versions 2025.11.7 and 2026.1.3; organizations that cannot upgrade can apply the security patch plugin to TeamCity 2017.1 and later. Restrict network access to trusted systems as defense-in-depth. TeamCity Cloud users are not required to take any action.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-63077	JetBrains TeamCity On-Premises (all versions before 2025.11.7 and before 2026.1.3)	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*:*:*	CWE-502

Recommendations

Update TeamCity Immediately: Upgrade all TeamCity On-Premises servers to a fixed release, either 2025.11.7 or 2026.1.3, using the vendor download page or the built-in automatic update option. This is the definitive remediation and, given the KEV listing and active-exploitation designation, it should be treated as an urgent, out-of-cycle change.

Apply the Security Patch Plugin Where Upgrades Are Not Possible: For environments running TeamCity 2017.1 or later that cannot upgrade immediately, install the vendor-provided security patch plugin, which addresses this specific vulnerability. Note that the plugin remediates only CVE-2026-63077 and is a stopgap; a full upgrade remains necessary to receive other security fixes. Servers on 2017.1 to 2018.1 require a restart after installation, while 2018.2 and later can enable the plugin without a restart.

Restrict Network Exposure of TeamCity Servers: As a defense-in-depth measure, limit network access to TeamCity servers to trusted networks and required systems only, for example by requiring VPN access or placing the server behind network segmentation, and restrict reachability of the agent polling port to known agent address ranges. Even exposing the login screen or REST API offers attackers an entry point for newly disclosed flaws.

Hunt for Signs of Compromise: Because the vulnerability is under active exploitation, assume exposed servers may already have been targeted and proactively hunt for indicators of post-exploitation activity. Review for unexpected child processes spawned by the TeamCity server process, particularly shells, scripting interpreters, or download utilities; outbound connections from the server to unfamiliar destinations following inbound polling traffic; unauthorized build configurations, plugins, or scheduled tasks; and new or anomalous service accounts on the host.

Rotate Potentially Exposed Secrets: If compromise is suspected or cannot be ruled out on a previously exposed server, rotate all credentials, access tokens, and signing keys stored in or accessible to the TeamCity server, since credential exposure is an explicitly documented consequence of successful exploitation.

Enforce Least Privilege and Host Isolation: Run the TeamCity server with the minimum operating system privileges required for normal operation and on dedicated hosts kept separate from build agents. This constrains the impact of any successful exploitation, which executes with the privileges of the server process.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
Execution	T1059: Command and Scripting Interpreter	
Credential Access	T1552: Unsecured Credentials	

Patch Links

https://www.jetbrains.com/teamcity/download/other.html

https://download.jetbrains.com/teamcity/plugins/internal/fix_CVE_2026_63077.zip

References

https://blog.jetbrains.com/teamcity/2026/07/cve-2026-63077/

https://www.sentinelone.com/vulnerability-database/cve-2026-63077/

https://www.rapid7.com/blog/post/etr-cve-2026-63077-critical-unauthenticated-remote-code-execution-in-jetbrains-teamcity/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

August 07, 2026 • 11:30 AM

More at www.hivepro.com