Update: Critical Remote Code Execution Vulnerability in JetBrains TeamCity On-Premises (CVE-2026-63077)

Sep 28, 2026

View Alert

WHITE

JetBrains has released security fixes for an unauthenticated remote code execution vulnerability (CVE-2026-63077) affecting all customer-managed TeamCity On-Premises installations.

The flaw allows remote attackers with network access over HTTP or HTTPS to bypass authentication checks and execute arbitrary operating system commands on the underlying server. While JetBrains has already automatically patched its fully managed cloud service, administrators responsible for self-hosted customer-managed servers must apply software updates or install the security patch plugin.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their risk exposure to this vulnerability.

Update (as of September 28, 2026): Ransomware groups are now exploiting this critical vulnerability. Meanwhile, security threat watchdog Shadowserver is still tracking over 160 TeamCity servers that are unpatched against the flaw.

Additional Info

Analysis:

CVE-2026-63077 is an unauthenticated authentication bypass flaw in the TeamCity agent polling protocol for servers reachable via HTTP or HTTPS. A third-party security researcher privately reported the vulnerability to JetBrains on July 10, 2026, under coordinated vulnerability disclosure. Because the flaw stems from how the server validates incoming agent polling protocol interactions, a remote attacker can exploit it to bypass server authentication checks without valid user credentials or an existing session.

Exploiting this vulnerability enables an attacker to achieve remote code execution with the exact operating system privileges of the TeamCity server process. Depending on those process permissions, successful exploitation allows an adversary to exfiltrate TeamCity data, stored credentials, and configuration files, and to alter server state. Because CI/CD infrastructure orchestrates core deployment pipelines, compromising the server process also introduces significant risk to downstream build artifacts and the integrity of the software supply chain.

Evaluating risk requires understanding the distinction between software deployment models. The vulnerability strictly impacts TeamCity On-Premises, which refers to the customer-managed software edition administered by an organization on its local physical hardware, internal private clouds, or public cloud platform virtual machines. Conversely, JetBrains TeamCity Cloud refers to the fully managed software-as-a-service platform hosted by JetBrains, where JetBrains engineers have already applied the necessary mitigations across all environments and confirmed there is no evidence of active exploitation.

JetBrains has addressed CVE-2026-63077 by releasing updated software versions alongside a standalone security patch plugin for legacy installations. Organizations can resolve the issue by updating self-hosted servers to version 2025.11.7 or 2026.1.3. For customer-managed environments unable to perform a full server upgrade immediately,

JetBrains released a security patch plugin compatible with TeamCity 2017.1 and newer, allowing organizations to fix the flaw without a full platform upgrade.

Recommendations and Mitigations:

Health-ISAC recommends organizations review and assess their risk exposure to this vulnerability and implement the following:

- Upgrade self-hosted servers to version 2025.11.7 or 2026.1.3 via direct download or internal update utilities.
- For customer-managed environments running TeamCity 2017.1 or newer that cannot perform an immediate full upgrade, install the official CVE-2026-63077 security patch plugin:
    - TeamCity 2024.03+: Review and apply the automatically fetched patch under Administration > Updates > Available security updates.
    - TeamCity 2017.1 to 2018.1: Restart the TeamCity server process after installing the plugin to complete activation.
    - TeamCity 2018.2+: Enable the plugin directly via the console without requiring a server restart.
- Verify whether your organization uses vendor-hosted TeamCity Cloud or customer-managed TeamCity On-Premises.
- Limit direct internet access to TeamCity login screens and REST APIs by placing servers behind trusted internal networks or requiring VPN access.
- Run the TeamCity server process using a low-privileged operating system account to limit post-exploitation lateral movement and ensure build agents remain isolated on dedicated hosts.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

<hr size=1 width="100%" align=center>

Alert Id	ab764b1d
Category	Threat Bulletins
References	thehackernews hhs helpnetsecurity jetbrains 1 bleepingcomputer shadowserver
Tags	CVE-2026-63077, TeamCity, JetBrains

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Please provide your feedback

Like Dislike

Download the App

Available on iOS, Android and Web

Download on the App Store Get it on Google Play

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--
You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.
To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.
To view this discussion visit https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a0e65a3f49-1a234701-b3d9-417a-8c91-60b00e4d3243-000000%40email.amazonses.com.