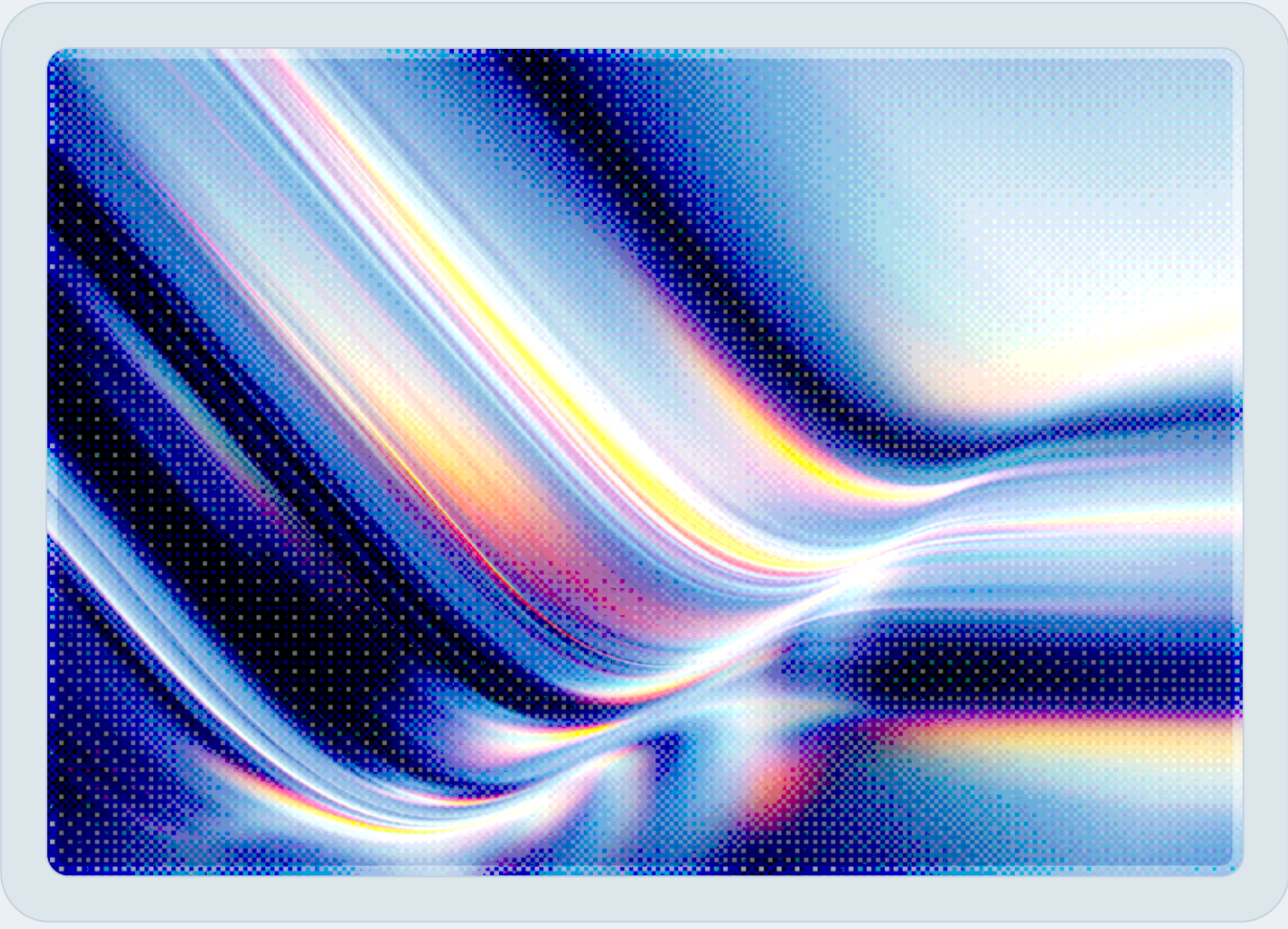
CSAI Foundation | Cloud Security Alliance

CISA's TeamCity KEV Addition: A Three-Day Deadline

CVE-2026-63077 and the CI/CD Supply Chain

2026-08-06

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

CISA added CVE-2026-63077, a critical unauthenticated remote code execution flaw in JetBrains TeamCity On-Premises, to its Known Exploited Vulnerabilities (KEV) catalog on August 5, 2026, and set a federal remediation deadline of August 8, 2026 [1][2]. The three-day window is not an outlier: it reflects CISA's Binding Operational Directive (BOD) 26-04, issued June 10, 2026, which replaces flat CVSS-based deadlines with a four-variable risk model and assigns its shortest tier to vulnerabilities that are internet-exposed, KEV-listed, capable of automated exploitation, and rated for full technical compromise [3]. CVE-2026-63077 meets the technical-impact, KEV-status, and automation criteria outright: it carries a CVSS score of 9.8, requires no authentication, and grants an attacker arbitrary operating-system command execution with the privileges of the TeamCity server process [4][5]. It also meets the exposure criterion for the population of TeamCity deployments generally, since build servers are typically reachable by distributed build agents over the internet or broad internal networks, though public reporting has not yet quantified how many individual instances remain both unpatched and internet-facing. Because TeamCity servers sit at the center of the build-and-release pipeline, storing source access tokens, cloud credentials, signing material, and deployment secrets, a compromised instance functions less like a single-host incident and more like a foothold into every downstream system the pipeline touches [6]. Organizations running TeamCity On-Premises should treat the federal deadline as the outer bound of a defensible response timeline, not the standard to aim for, given that CISA's own criteria imply a threat already weaponized for speed.

Background

JetBrains disclosed CVE-2026-63077 on July 27, 2026, crediting security researcher Antoni Tremblay, who reported the flaw privately on July 10 in accordance with the company's coordinated disclosure process [5]. The vulnerability is a deserialization-of-untrusted-data issue (CWE-502) in the agent polling protocol that TeamCity build agents use to communicate with the server. An unauthenticated attacker with HTTP or HTTPS access to a vulnerable server can send a crafted request through that protocol, bypass authentication entirely, and execute arbitrary OS commands with the server process's privileges [4][5]. JetBrains fixed the issue in TeamCity 2025.11.7 and 2026.1.3, and published a standalone security patch plugin for organizations running older but still-supported releases back to

version 2017.1; servers on 2017.1 through 2018.1 must restart after applying the plugin, while 2018.2 and later can apply it without downtime [5]. TeamCity Cloud customers are not affected, since the vulnerable component exists only in the on-premises product [4][5].

At the time of disclosure, JetBrains had not identified evidence of exploitation in the wild. That changed within nine days: CISA added CVE-2026-63077 to the KEV catalog on August 5, confirming active exploitation, though the agency's alert does not name a specific threat actor, describe the exploitation technique observed, or estimate the scale of affected servers [1][2][7]. The compressed gap between disclosure (July 27) and confirmed in-the-wild exploitation (on or before August 5) is consistent with the rationale CISA cited for BOD 26-04: proof-of-concept code for high-value, unauthenticated vulnerabilities in developer-facing infrastructure is increasingly weaponized within days rather than weeks [3].

This is also not the first time a TeamCity vulnerability has drawn this level of federal urgency. In December 2023, CISA, the FBI, the NSA, and allied agencies in Poland and the United Kingdom issued a joint advisory attributing large-scale exploitation of an earlier critical TeamCity authentication-bypass flaw, CVE-2023-42793, to Russia's Foreign Intelligence Service (APT29, also tracked as Midnight Blizzard or Cozy Bear), which used compromised servers to pursue software supply chain access [8]. That episode is the reason security teams should not read CVE-2026-63077 as a routine patch-cycle item: unauthenticated RCE in TeamCity has previously drawn the attention of a sophisticated, state-sponsored actor (APT29, in 2023) specifically because of what the platform enables downstream, not merely because of the CVSS score attached to any single flaw.

The table below summarizes the core facts of the vulnerability for teams that need to brief leadership or triage against an asset inventory quickly.

Attribute	Detail
CVE	CVE-2026-63077
Product	JetBrains TeamCity On-Premises (all versions prior to fix)
CVSS score	9.8 (Critical)
Vulnerability class	Deserialization of untrusted data (CWE-502) in the agent polling protocol
Authentication required	None
Impact	Arbitrary OS command execution as the TeamCity server process

Attribute	Detail
Disclosed	July 27, 2026 (JetBrains advisory)
Added to CISA KEV	August 5, 2026
Federal remediation deadline	August 8, 2026
Fixed versions	2025.11.7 and 2026.1.3
Interim mitigation	JetBrains security patch plugin (TeamCity 2017.1+)
TeamCity Cloud	Not affected

Security Analysis

Why This Vulnerability Cleared CISA's Shortest Tier

BOD 26-04 scores vulnerabilities against four binary conditions — public exposure of the affected asset, presence in the KEV catalog, whether exploitation can be automated, and whether successful exploitation produces high-severity technical impact — and reserves its three-day remediation tier for vulnerabilities meeting all four [3]. CVE-2026-63077 meets that bar cleanly. TeamCity servers are commonly deployed with internet-facing access so that distributed build agents can reach them, which is why the exposure criterion is plausibly met for a meaningful share of deployments, though, as discussed below, no public data yet quantifies how many internet-facing instances remain unpatched. The KEV listing itself satisfies the second criterion. The vulnerability requires no authentication and no user interaction, which makes it straightforward to script and scan for at scale, satisfying the automation criterion. And the technical impact is total: arbitrary OS command execution with server-process privileges gives an attacker read access to stored credentials, the ability to modify server configuration, and the ability to tamper with build outputs before they reach production [4][6]. CSA's analysis of BOD 26-04 noted that this four-variable model was designed precisely to separate vulnerabilities like this one, where every factor compounds risk, from lower-urgency CVEs that happen to carry a high CVSS score in isolation [3].

The CI/CD Blast Radius

The practical danger of a TeamCity compromise extends well past the server itself. Build systems function as a trust anchor for everything they produce: if an attacker can read the credentials TeamCity holds or alter the commands a build executes, they can potentially inject malicious code into artifacts that are later signed, deployed, and trusted by every downstream consumer of that software. CSA's research on the 2025–2026 wave of CI/CD and developer-tooling intrusions documented a cascading credential-reuse pattern, in which compromise of one build-adjacent tool provided the credentials needed to compromise the next tool in the pipeline, expanding the population of affected organizations with each stage [9]. TeamCity's role as a central credential store for build-and-release infrastructure places a compromised instance at the same entry point CSA identified as the trigger for that cascade: a single point of initial credential theft with the potential to propagate outward. A build server compromised through CVE-2026-63077 is a plausible entry point for exactly this kind of cascading intrusion, in which the attacker's real objective is not the TeamCity host but the software supply chain it feeds.

An Open Question on Scale

Public reporting to date has not disclosed how many internet-facing TeamCity On-Premises servers remain unpatched, nor has it detailed the specific tactics, techniques, and procedures observed in confirmed exploitation [7]. Security vendors with internet-scanning visibility, including Rapid7, have published detection guidance and vulnerability checks but likewise stop short of exposure counts [7]. This absence of public telemetry means organizations cannot rely on "it's probably not widespread" as a risk-acceptance rationale; the KEV listing itself is CISA's attestation that exploitation is confirmed, and the lack of published scale data should be read as an information gap, not as reassurance.

Recommendations

Immediate Actions

Organizations running TeamCity On-Premises should identify every instance in their environment, including shadow or team-managed installations outside central IT's inventory, and confirm the version against 2025.11.7 and 2026.1.3. Any instance below those versions should be patched or upgraded within the federal deadline of August 8, and organizations that cannot upgrade immediately should apply JetBrains' interim security patch plugin, which is available back to TeamCity 2017.1 [5]. Given that exploitation is already confirmed, teams should also perform forensic triage before or alongside

patching, reviewing TeamCity server logs, credential stores, and recent build artifacts for signs of prior compromise, rather than assuming that patching alone restores a clean state, consistent with CISA's own guidance under BOD 26-04 that high-tier vulnerabilities warrant compromise assessment ahead of remediation [3].

Short-Term Mitigations

Beyond patching, organizations should restrict network exposure of TeamCity servers to the minimum set of build agents and administrators that require access, removing direct internet exposure where it is not operationally necessary. Credentials and tokens accessible to the TeamCity server, including source control tokens, cloud provider keys, and code-signing material, should be rotated as a precaution, since a server that was compromised prior to patching may have already exposed them. Build and deployment logs from the weeks surrounding disclosure should be reviewed for anomalous administrative actions, unexpected build configuration changes, or artifacts published outside normal release windows.

Strategic Considerations

Organizations that have not yet mapped their internet-exposed assets against CISA's four-variable risk model should treat this incident as a forcing function to do so, since BOD 26-04's shortest tier will keep applying to whichever developer-facing infrastructure meets all four criteria next [3]. More broadly, this event reinforces that CI/CD platforms, package registries, and developer tooling now sit inside the trust boundary that security programs must actively defend, not at its perimeter. Aligning credential issuance for build systems with short-lived, least-privilege access rather than long-lived static tokens, and building the internal capability to perform rapid forensic triage on build infrastructure, will reduce both the likelihood and the blast radius of the next unauthenticated RCE in a CI/CD tool.

CSA Resource Alignment

CSA's research on the 2025–2026 wave of CI/CD and developer-tooling supply chain intrusions, *TeamPCP: Cascading Supply Chain Assault via Developer Security Tooling*, documented how compromise of a single build-adjacent tool cascaded into credential theft and downstream software supply chain exposure across multiple organizations — the same blast-radius dynamic that makes CVE-2026-63077 significant beyond the TeamCity host itself [9]. CSA's analysis of the directive that set this vulnerability's remediation deadline, *CISA BOD 26-04: AI Threat Forces 3-Day Critical Patch Mandate*, explains the four-variable risk model in detail and argues that its shortest tier is being driven by AI-accelerated exploit weaponization compressing the gap between disclosure and active exploitation, precisely the pattern

this vulnerability followed [3]. CSA's follow-up analysis, *From Executive Order to Enforcement: BOD 26-04's Patch Signal*, documents how quickly CISA operationalized the directive and highlights persistently low real-world remediation rates for KEV-listed vulnerabilities, a gap this incident suggests will keep recurring for internet-facing developer infrastructure that meets BOD 26-04's shortest-tier criteria [10]. Finally, CSA's AI Controls Matrix (AICM v1.1) offers a broader control framework, spanning 247 control objectives across 18 security domains including identity and access management, that organizations can use to structure defenses against build-server compromise generally, independent of this specific CVE [11].

References

[1] The Hacker News. "CISA Flags TeamCity CVE-2026-63077 RCE Flaw Under Active Exploitation in the Wild." The Hacker News, August 2026.

[2] Cybersecurity and Infrastructure Security Agency. "CISA Adds One Known Exploited Vulnerability to Catalog." CISA, August 5, 2026.

[3] Cloud Security Alliance. "CISA BOD 26-04: AI Threat Forces 3-Day Critical Patch Mandate." CSA AI Safety Initiative, June 2026.

[4] Rapid7. "CVE-2026-63077: Critical Unauthenticated Remote Code Execution in JetBrains TeamCity." Rapid7 Blog, July 2026.

[5] JetBrains. "Critical Security Issue Affecting TeamCity On-Premises (CVE-2026-63077) – Update to 2025.11.7 or 2026.1.3 Now." The JetBrains Blog, July 27, 2026.

[6] Help Net Security. "JetBrains Fixes Critical Unauthenticated RCE in TeamCity On-Premises (CVE-2026-63077)." Help Net Security, July 28, 2026.

[7] Cybersecurity and Infrastructure Security Agency. "Known Exploited Vulnerabilities Catalog." CISA, accessed August 2026.

[8] Cybersecurity and Infrastructure Security Agency. "Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally (AA23-347A)." CISA, FBI, NSA, and international partners, December 13, 2023.

[9] Cloud Security Alliance. "TeamPCP: Cascading Supply Chain Assault via Developer Security Tooling." CSA AI Safety Initiative, April 2026.

[10] Cloud Security Alliance. "From Executive Order to Enforcement: BOD 26-04's Patch Signal." CSA AI Safety Initiative, July 2026.

[11] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2026.

© 2026 Cloud Security Alliance. AI-assisted Rapid Research.