March 5, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that JetBrains published a security advisory to address vulnerabilities in the following product:

- JetBrains TeamCity On-Premises – versions prior to 2023.11.4

Technical Details
Two new critical security vulnerabilities have been discovered in TeamCity On-Premises. If abused, the flaws may enable an unauthenticated attacker with HTTP(S) access to a TeamCity server to bypass the authentication checks and gain administrative control of the TeamCity server.

All versions of TeamCity On-Premises are affected by these vulnerabilities. Customers of TeamCity Cloud have already had their servers patched, and we have verified that they weren't attacked.

These vulnerabilities were discovered in February 2024 by Rapid7, who reported the vulnerabilities to us privately via our coordinated disclosure policy.

These two critical security vulnerabilities have been assigned the Common Vulnerabilities and Exposures (CVE) identifiers CVE-2024-27198 and CVE-2024-27199**,** and present the weaknesses CWE-288 and CWE-23.

Fixes for these vulnerabilities have been introduced in version 2023.11.4. We have also released a security patch plugin so that customers who are unable to upgrade to this version can still patch their environment.

.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-27198 and CVE-2024-27199
- JetBrains Security Advisory
- JetBrains Fixed Security Issues