Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

JetBrains TeamCity Authentication Bypass Flaw, Paving the Way for Server Takeover

Date of Publication	Admiralty Code	TA Number
February 8, 2024	A1	TA2024049

Summary

First Seen: January 19, 2024
Affected Products: TeamCity On-Premises
Impact: JetBrains addressed a critical security flaw in its TeamCity On-Premises product. The vulnerability identified as CVE-2024-23917, could potentially allow an unauthorized attacker with HTTP(S) access to a TeamCity server to circumvent authentication mechanisms and acquire administrative privileges over the affected server.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-23917	JetBrains TeamCity Authentication Bypass Vulnerability	TeamCity	☒	☒	✓

Vulnerability Details

#1 JetBrains has urged the customers to promptly apply patches to their TeamCity On-Premises servers to mitigate a critical vulnerability identified as CVE-2024-23917. This vulnerability could potentially allow attackers to exploit an authentication bypass flaw, enabling them to gain administrative control over vulnerable instances.

#2 Vulnerability CVE-2024-23917 poses a significant risk as it allows remote attackers to compromise the affected system. This vulnerability stems from a flaw in the authentication process, enabling attackers to bypass authentication checks and seize administrative control over the TeamCity server.

#3 This critical security vulnerability impacts all versions of TeamCity On-Premises ranging from 2017.1 to 2023.11.2. To facilitate patching for environments unable to update to version 2023.11.3, JetBrains has developed a security patch plugin with installation instructions.

#4 While JetBrains asserts that all TeamCity Cloud servers have been patched and no evidence of an attack has been found, they have not disclosed whether CVE-2024-23917 has been exploited in the wild to compromise TeamCity On-Premises servers accessible over the Internet.

#5 Since early October 2023, threat actors have been exploiting a similar authentication bypass issue in TeamCity, known as CVE-2023-42793, which also enabled remote code execution (RCE) attacks. These groups were found to be deploying backdoors through this vulnerability, and their activities were likely aimed at conducting software supply chain attacks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-23917	TeamCity: 2017.1 - 2023.11.2	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*:*	CWE-288

Recommendations

Apply Patch: Install the security patch provided by JetBrains to address the CVE-2024-23917 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on TeamCity servers. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application		

Patch Details

JetBrains has released patches for this vulnerability in the following version: 2023.11.3

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

If updating your server to version 2023.11.3 is not feasible, update the security patch plugin,
For version 2018.2 and above
Link:
https://download.jetbrains.com/teamcity/plugins/internal/fix_CVE_2024_23917.zip

For version 2017.1, 2017.2, and 2018.1
Link:
https://download.jetbrains.com/teamcity/plugins/internal/fix_CVE_2024_23917_pre2018_2.zip

References

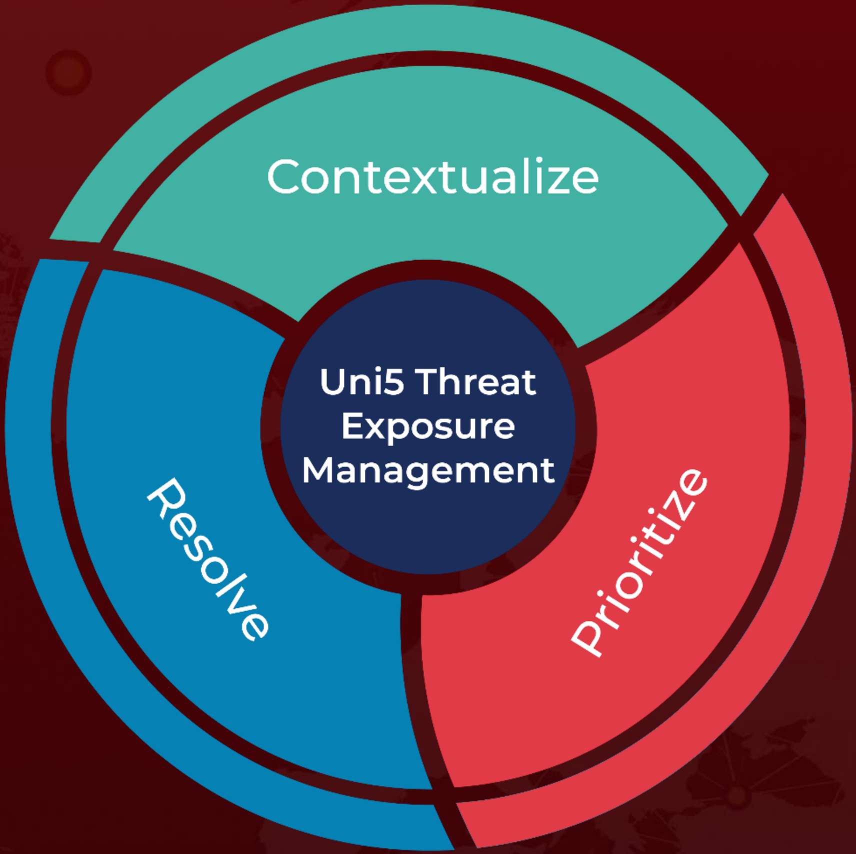
https://blog.jetbrains.com/teamcity/2024/02/critical-security-issue-affecting-teamcity-on-premises-cve-2024-23917/

https://www.hivepro.com/threat-advisory/north-korean-actors-behind-active-exploitation-of-teamcity-vulnerability/

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 8, 2024 • 4:45 AM

More at www.hivepro.com