Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Vulnerabilities Discovered in TeamCity, Enable Server Takeover

Date of Publication	Last Update Date	Admiralty Code	TA Number
March 5, 2024	March 8, 2024	A1	TA2024085

Summary

First Seen: February 2024
Affected Products: TeamCity On-Premises
Impact: Two vulnerabilities in the JetBrains TeamCity On-Premises software have been discovered (CVE-2024-27198 and CVE-2024-27199). Threat actors may attempt to take advantage of these vulnerabilities in order to breach and gain control of the impacted systems leading to system compromise.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-27198	JetBrains TeamCity Authentication Bypass Vulnerability	TeamCity On-Premises	✗	✓	✓
CVE-2024-27199	JetBrains TeamCity Path Traversal Vulnerability	TeamCity On-Premises	✗	✗	✓

Vulnerability Details

#1 Two critical security flaws in TeamCity On-Premises have been discovered tracked as CVE-2024-27198 and CVE-2024-27199. Due to these flaws, an unauthorised user having HTTP(S) access to a TeamCity server can circumvent security measures and take over the server's administration. These flaws affect all versions of TeamCity On-Premises up to 2023.

#2 The CVE-2024-27198 vulnerability found in TeamCity's web component allows unauthorized users to access endpoints that typically require authentication. Exploiting this flaw, remote and unauthenticated attackers can seize control of the server by crafting URLs that bypass authentication checks. To get complete control over the target server, this flaw could be leveraged for the creation of a new administrator account or obtain an administrator access token.

#3 The high-severity vulnerability CVE-2024-27199 affects the web-based component of TeamCity and permits authentication bypass. This vulnerability allows unauthorized users to change system settings and gain access to private information. An attacker can change port numbers, add new HTTPS certificates, and cause denial-of-service (DoS) attacks on the server. This can be done by changing the HTTPS port number or submitting a certificate that is rejected by client-side validation.

#4 CVE-2024-27198 is being actively exploited in the wild, with exploit code documented on public sites. Exploitation attempts were observed after the vulnerability disclosure and by March 6, there were 1,700 vulnerable instances of TeamCity, with 1,400 of them showing clear indications of unauthorized user creation. CISA has included this vulnerability in its KEV catalog, setting the patch due date for March 28th.

#5 Patches are now released in Version 2023.11.4 for these vulnerabilities. Additionally, to assist users who cannot update to this version promptly, a security patch plugin for version 2018.2 and 2018.1 has been made available.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-27198	TeamCity On-Premises versions upto 2023.11.3	cpe:2.3:a:jetbrains:TeamCity:*:*:*:*:*:*:*:*	CWE-288
CVE-2024-27199	TeamCity On-Premises versions upto 2023.11.3	cpe:2.3:a:jetbrains:TeamCity:*:*:*:*:*:*:*:*	CWE-23

Recommendations

Apply Patch & Update Server: Install the security patch and update your server to the latest version 2023.11.4 provided by JetBrains TeamCity to address the CVE-2024-27198 and CVE-2024-27199 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Validate Installed Plugin and Review System Logs: It's essential to thoroughly scrutinize any plugin which is present in the system to ensure it's not malicious. Review system logs located at /opt/TeamCity/logs/ in Linux installations and C:\TeamCity\logs\ in windows installations for tracing any malicious activity. Validate these logs for abnormal events related to malicious plugin upload, system tampering and new account creation.

Regular Audits and Reviews: Conduct regular audits and reviews of user accounts to ensure that all admin accounts are legitimate and authorized. This can help identify any unauthorized account creations.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation
TA0040 Impact	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1136 Create Account
T1608 Stage Capabilities	T1608.003 Install Digital Certificate	T1498 Network Denial of Service	T1556 Modify Authentication Process
T1190 Exploit Public-Facing Application	T1134 Access Token Manipulation	T1134.003 Make and Impersonate Token	

Patch Details

JetBrains has released patches for these vulnerabilities in the latest version 2023.11.4

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

References

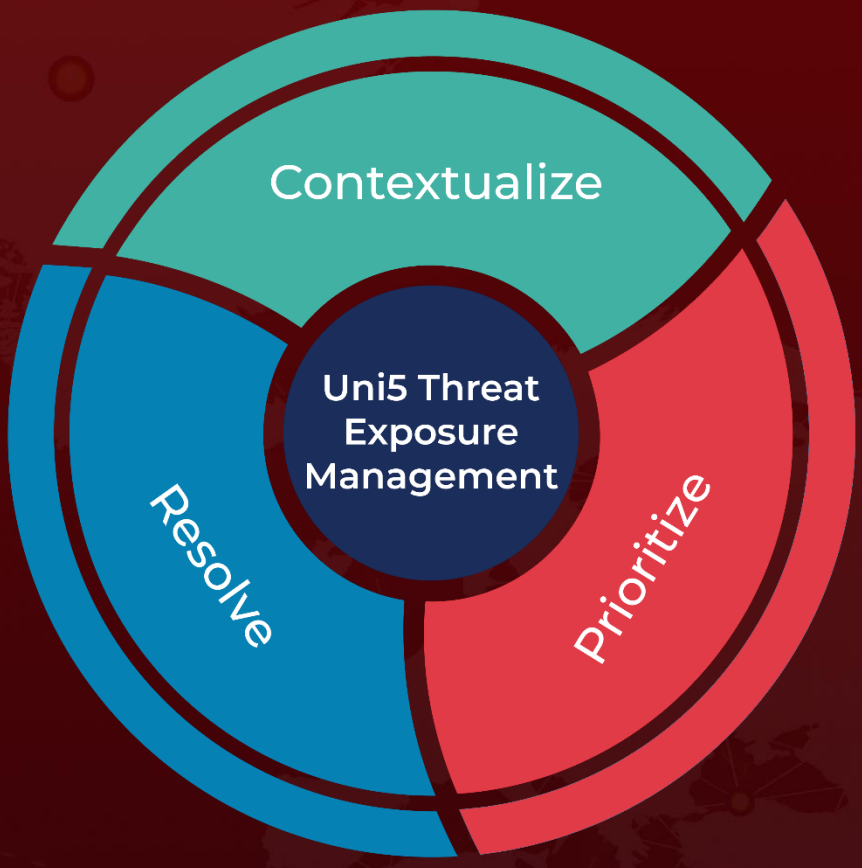
https://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now/

https://www.rapid7.com/blog/post/2024/03/04/etr-cve-2024-27198-and-cve-2024-27199-jetbrains-teamcity-multiple-authentication-bypass-vulnerabilities-fixed/

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

March 5, 2024 • 5:45 AM

More at www.hivepro.com