مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in JetBrains TeamCity On-Premises Software

Tracking #:432315667

Date:05-03-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Critical Vulnerabilities in JetBrains TeamCity On-Premises software that could be exploited to gain complete control of affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

1. CVE-2024-27198 (CVSS score: 9.8 - Critical): An authentication bypass vulnerability in the web component of TeamCity arising from an alternative path issue (CWE-288). This vulnerability allows an attacker to gain complete control over a vulnerable TeamCity On-Premises server, including for remote code execution.

- Compromising a TeamCity server allows an attacker full control over all TeamCity projects, builds, agents and artifacts, and as such is a suitable vector to position an attacker to perform a supply chain attack.

2.CVE-2024-27199 (CVSS score: 7.3 - High): An authentication bypass vulnerability in the web component of TeamCity arising from a path traversal issue (CWE-22). This vulnerability could allow an unauthenticated attacker to perform limited information disclosure and system modifications, including replacing the HTTPS certificate on a vulnerable TeamCity server.

- A threat actor could leverage the vulnerability to perform a denial-of-service attack against the TeamCity server by either changing the HTTPS port number or uploading a certificate that fails client-side validation. Alternatively, the uploaded certificate could be used for man-in-the-middle attacks if it's trusted by the clients.

Affected Products:
TeamCity On-Premises versions through 2023.11.3.

Fixed Versions:
TeamCity On-Premises versions through 2023.11.4.

If unable to update to version 2023.11.4, a security patch plugin is available for TeamCity 2018.2 and newer, and for TeamCity 2018.1 and older.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by JetBrains.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

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/