Security Advisory 2024-023

Vulnerabilities in JetBrains TeamCity

March 6, 2024 — v1.0

TLP:CLEAR

History:

- *06/03/2024 — v1.0 – Initial publication*

Summary

On March 4, JetBrains released a fix for two vulnerabilities affecting JetBrains TeamCity CI/CD server. Both vulnerabilities are authentication bypass vulnerabilities. If exploited, the most severe vulnerability allows for a complete compromise of a vulnerable TeamCity server by a remote unauthenticated attacker, including unauthenticated RCE [1,2].

It is advised upgrading the software as soon as possible.

Technical Details

The vulnerability **CVE-2024-27198**, with a CVSS score of 9.8, is an authentication bypass vulnerability in the web component of TeamCity that arises from an alternative path issue. TeamCity exposes a web server over HTTP port 8111 by default (and can optionally be configured to run over HTTPS). An attacker can craft a URL such that all authentication checks are avoided, allowing endpoints that are intended to be authenticated to be accessed directly by an unauthenticated attacker. A remote unauthenticated attacker can leverage this to take complete control of a vulnerable TeamCity server.

The vulnerability **CVE-2024-27199**, with a CVSS score of 7.3, is an authentication bypass vulnerability in the web component of TeamCity that arises from a path traversal issue. This authentication bypass allows for a limited number of authenticated endpoints to be reached without authentication. An unauthenticated attacker can leverage this vulnerability to both modify a limited number of system settings on the server, as well as disclose a limited amount of sensitive information from the server.

Affected Products

All versions of TeamCity On-Premises with a version prior 2023.11.4 are affected by these vulnerabilities. For customers with TeamCity Cloud, JetBrains patched the servers and verified that no exploitation of these vulnerabilities were initiated.

Recommendations

CERT-EU strongly recommends updating software installations to the latest versions by following the instructions given by the vendor [1,2].

Detection

To detect exploitation activities, it is recommended reviewing the web access logs and the software logs [1], by default located in `C:\TeamCity\logs\` on Windows and `/opt/TeamCity/logs/` on Linux.

- An attacker could leverage the vulnerabilities to create a new access token for persistence. In that case, a log entry in the `teamcity-javaLogging` log files would indicate such activity. By searching for strings matching the following regular expression in those log files, one could find succesful exploitation attempts: `;\S*\.jsp\?\S*jsp=`, and `\/\S*\?\S*jsp=\S*;\.jsp`.

```
27-Feb-2024 07:15:45.191 WARNING [TC: 07:15:45 Processing REST request; http-nio-80-exec-5]
  com.sun.jersey.spi.container.servlet.WebComponent.filterFormParameters A servlet request, to
  the URI http://xxx.xxx.xxx.xxx/app/rest/users/id:1/tokens/wo4qEmUZ;O.jsp?WkBR=OcPj9HbdUcKxH3O
  &pKLaohp7=dOjMHTumGred&jsp=/app/rest/users/id%3a1/tokens/wo4qEmUZ%3bO.jsp&ja7U2Bd=nZLi6Ni,
  contains form parameters in the request body but the request body has been consumed by the
  servlet or a servlet filter accessing the request parameters. Only resource methods using
  @FormParam will work as expected. Resource methods consuming the request body by other means
  will not work as expected.
```

- An attacker could leverage the vulnerabilities to upload malicious plugin. In that case, a log entry in the `teamcity-server.log` and the `teamcity-activities.log` log files would indicate such activity. By searching for lines indicating that a plugin was uploaded and subsequently deleted in quick succession, and authenticated with the same user account as that of the initial access token creation, one could find succesful exploitation attempts.

```
[2024-02-26 07:11:13,304]   INFO - s.buildServer.ACTIVITIES.AUDIT - plugin_uploaded: Plugin
  "WYyVNA6r" was updated by "user with id=1" with comment "Plugin was uploaded to
  C:\ProgramData\JetBrains\TeamCity\plugins\WYyVNA6r.zip"
[2024-02-26 07:11:24,506]   INFO - s.buildServer.ACTIVITIES.AUDIT - plugin_disable: Plugin
  "WYyVNA6r" was disabled by "user with id=1"
[2024-02-26 07:11:25,683]   INFO - s.buildServer.ACTIVITIES.AUDIT - plugin_deleted: Plugin
  "WYyVNA6r" was deleted by "user with id=1" with comment "Plugin was deleted from
  C:\ProgramData\JetBrains\TeamCity\plugins\WYyVNA6r.zip"
```

- An attacker could leverage the vulnerabilities to create an administrator account. In that case, a log entry in the in the `teamcity-server.log` and the `teamcity-activities.log` log files would indicate such activity. It is also possible to review the TeamCity administration console's Audit page for newly created accounts.

```
[2024-02-26 07:45:06,962]   INFO - tbrains.buildServer.ACTIVITIES - New user created: user with
   id=23
[2024-02-26 07:45:06,962]   INFO - s.buildServer.ACTIVITIES.AUDIT - user_create: User "user
  with id=23" was created by "user with id=23"
```

- To find exploitation of the second exploitation, one can search for double dot path segments (i.e., `../`), in the web access logs, after the the follwing vulnerable paths: `/res/`, `/update/`, and `/.well-known/acme-challenge/`.

References

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

[2] 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/