



# CVE-2022-24335

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-24335
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-25 15:15:00 UTC
<b>Updated</b>	2022-03-04 02:23:00 UTC
<b>Description</b>	JetBrains TeamCity before 2021.2 was vulnerable to a Time-of-check/Time-of-use (TOCTOU) race-condition attack in ager

## Risk And Classification

**Problem Types:** CWE-367

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jetbrains	Teamcity	All	All	All	All

## References

Reference	Source	Link	Tags
The JetBrains Blog   Developer Tools for Professionals and Teams	MISC	<a href="https://blog.jetbrains.com">blog.jetbrains.com</a>	
JetBrains Security Bulletin Q4 2021   JetBrains News	MISC	<a href="https://blog.jetbrains.com">blog.jetbrains.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**