

Department of the Environment, Climate & Communications

---



## NCSC Alert

---

### Multiple Vulnerabilities in JetBrains TeamCity

Thursday 21<sup>st</sup> September, 2023

**STATUS: TLP-CLEAR**

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP-CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP-CLEAR** information may be shared without restriction. For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>. Please treat this document in accordance with the TLP assigned.*

## Description

JetBrains has released a software update for their TeamCity product that addresses the vulnerabilities [CVE-2023-42793](#) and [CVE-2023-43566](#). CVE-2023-42793 is a critical severity authentication bypass vulnerability with a CVSS score of 9.8. Exploitation of CVE-2023-42793 could lead to a remote code execution (RCE) attack. CVE-2023-43566 is stored XSS vulnerability, that can occur during a Teamcity node configuration.

## Products Affected

TeamCity is a build management and continuous integration server from JetBrains. CVE-2023-42793 and CVE-2023-43566 affect TeamCity versions prior to:

- 2023.05.4.

## Impact

Exploitation of CVE-2023-42793 can be used for authentication bypass leading to RCE on TeamCity servers, allowing an attacker to execute arbitrary code, which could result in system compromise and data loss.

## Recommendations

The NCSC strongly advises affected organisations to upgrade TeamCity servers to the remediated version as soon as possible and keep up to date with any further JetBrains security updates. Exposing systems to the internet significantly increases the risk against that system and networks connected to that system. Services should not be exposed to the internet unless strictly necessary.

Further information can be found here:

- [JetBrains - Fixed Security Issues in TeamCity](#)
- [NIST CVE-2023-42793](#)
- [NIST CVE-2023-43566](#)

**DISCLAIMER:** This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre  
29-31 Adelaide Road,  
Dublin, D02 X285,  
Ireland  
**Tel:** +353 (0)1 6782333  
**Mail:** [certreport@decc.gov.ie](mailto:certreport@decc.gov.ie)  
**Web:** [ncsc.gov.ie](http://ncsc.gov.ie)  
**Twitter:** [ncsc\\_gov\\_ie](https://twitter.com/ncsc_gov_ie)  
**LinkedIn:** [ncsc-ie](https://www.linkedin.com/company/ncsc-ie)

