National Cyber Security Centre

2309210159-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple Vulnerabilities in JetBrains TeamCity
UPDATE

Thursday 14th December, 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.

Revision History

Revision	Date	Author(s)	Description
1.0	21st September 2023	CSIRT-IE	Initial advisory
1.1	14th December 2023	CSIRT-IE	Update with details of exploitation and IOCs

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.

UPDATE: On December 14th further information was released with regards to observed exploitation of these vulnerabilities.

The U.S. Federal Bureau of Investigation (FBI), U.S. Cybersecurity & Infrastructure Security Agency (CISA), U.S. National Security Agency (NSA), Polish Military Counterintelligence Service (SKW), CERT Polska (CERT.PL), and the UK's National Cyber Security Centre (NCSC) has assessed that Russian Foreign Intelligence Service (SVR) cyber actors—also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and NOBELIUM/Midnight Blizzard—are exploiting **CVE-2023-42793** at a large scale, which they say have been targeting servers hosting JetBrains TeamCity software since September 2023.

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:

- CISA Indicators of Compromise
- 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@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie