



CVE-2019-15848

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

Summary

CVE	CVE-2019-15848
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-05 20:15:00 UTC
Updated	2019-09-18 14:15:00 UTC
Description	JetBrains TeamCity 2019.1 and 2019.1.1 allows cross-site scripting (XSS), potentially making it possible to send an arbitrar

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jetbrains	Teamcity	2019.1	-	All	All
Application	Jetbrains	Teamcity	2019.1.1	All	All	All
Application	Jetbrains	Teamcity	2019.1	-	All	All
Application	Jetbrains	Teamcity	2019.1.1	All	All	All

References

Reference

Jetbrains TeamCity Reflected XSS September 2019
Jonathan Leitschuh #BlackLivesMatter na Twitterze: "CVE-2019-15848: @teamcity (a tool similar to Jenkins) versions 2019.1 & 2019.1.1 are "
Full POC for CVE-2019-15848 · GitHub
Important Security Notice: XSS vulnerability allowing RCE The TeamCity Blog
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#).

Free CVE JSON API [cve.report/api](#)

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