

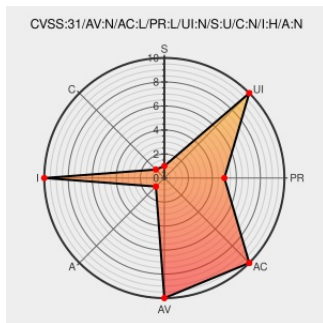


CVE-2021-26074

Published on: 04/15/2021 12:00:00 AM UTC

Last Modified on: 03/01/2022 04:25:00 PM UTC

CVE-2021-26074

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Connect Spring Boot](#) from [Atlassian](#) contain the following vulnerability:

Broken Authentication in Atlassian Connect Spring Boot (ACSB) from version 1.1.0 before version 2.1.3: Atlassian Connect Spring Boot is a Java Spring Boot package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Spring Boot app occurs with a server-to-server JWT or a context JWT.

Atlassian Connect Spring Boot versions from version 1.1.0 before version 2.1.3 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app.

CVE-2021-26074 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Atlassian](#) - **Atlassian Connect Spring Boot (ACSB)** version $\geq$ 1.1.0

Affected Vendor/Software: [Atlassian](#) - **Atlassian Connect Spring Boot (ACSB)** version $<$ 2.1.3

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

PARTIAL

NONE

CVE References

Description	Tags	Link
CVE-2020-26074 - Broken authentication in Atlassian Connect Spring Boot (ACSB) - Security - Atlassian Documentation	confluence.atlassian.com text/html	 N/A N/A
Action required: Atlassian Connect vulnerability allows bypass of app qsh verification via context JWTs - Announcements - The Atlassian Developer Community	community.developer.atlassian.com text/html	 MISC community.developer.atlassian.com/t/action-required-atlassian-connect-vulnerability-allows-bypass-of-app-qsh-verification-via-context-jwts/47072

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[982631](#) Java (maven) Security Update for com.atlassian.connect:atlassian-connect-spring-boot-starter (GHSA-cpcr-74q9-74gp)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Connect Spring Boot	All	All	All	All
cpe:2.3:a:atlassian:connect_spring_boot:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	cve.report/CVE-2021-26074 Broken Authentication in #Atlassian Connect Spring Boot ACSB from version 1.1.0 before v... twitter.com/i/web/status/1...	2021-04-16 19:52:14
 /r/netcve	CVE-2021-26074	2021-04-16 19:53:10

[← Previous ID](#)[Next ID →](#)

© CVE.report 2023   |

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](#).

