CVE-2021-26077

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-26077
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-10 00:15:00 UTC
Updated	2021-05-18 17:43:00 UTC
Description	Broken Authentication in Atlassian Connect Spring Boot (ACSB) in version 1.1.0 before 2.1.3 and from version 2.1.4 before

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Connect Spring Boot	All	All	All	All

References

Reference
Action required: Atlassian Connect vulnerability allows bypass of app qsh verification via context JWTs - Announcements - The Atlassian Deve
CVE-2021-26077 - Broken authentication in Atlassian Connect Spring Boot (ACSB) - Security - Atlassian Documentation
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982238 Java (maven) Security Update for com.atlassian.connect:atlassian-connect-spring-boot (GHSA-2x7v-w2mv-f3rx)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report