



CVE-2019-11581

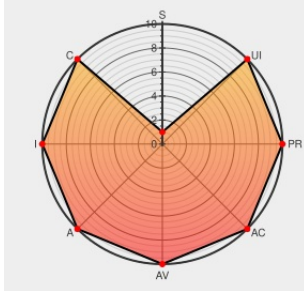
Published on: 08/09/2019 12:00:00 AM UTC

Last Modified on: 03/25/2022 05:22:00 PM UTC

CVE-2019-11581

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Jira](#) from [Atlassian](#) contain the following vulnerability:

There was a server-side template injection vulnerability in Jira Server and Data Center, in the ContactAdministrators and the SendBulkMail actions. An attacker is able to remotely execute code on systems that run a vulnerable version of Jira Server or Data Center. All versions of Jira Server and Data Center from 4.4.0 before 7.6.14, from 7.7.0

before 7.13.5, from 8.0.0 before 8.0.3, from 8.1.0 before 8.1.2, and from 8.2.0 before 8.2.3 are affected by this vulnerability.

CVE-2019-11581 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
UBASEDVED 605291 CVE 2019 11581 Template injection in various	CVE-2019-11581	MISC

[JRASERVER-69532] CVE-2019-11581 - Template injection in various resources - Create and track feature requests for Atlassian products.

Issue Tracking

Vendor Advisory

jira.atlassian.com

text/html

MISC

jira.atlassian.com/browse/JRASERVER-69532

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

730117 Atlassian Jira Server Template Injection Vulnerability (JRASERVER-69532)

Exploit/POC from Github

Atlassian JIRA Template injection vulnerability RCE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Jira	All	All	All	All
Application	Atlassian	Jira	All	All	All	All
Application	Atlassian	Jira Server	All	All	All	All
cpe:2.3:a:atlassian:jira:*:*:*:*:*:						
cpe:2.3:a:atlassian:jira:*:*:*:*:*:						
cpe:2.3:a:atlassian:jira_server:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @akkietech	3/25から毎日CVE-2019-11581(jiraのテンプレートインジェクションの脆弱性)を狙っていると見られる通信を検知している〜 GET /secure/ContactAdministrators!default.jspa HTTP/1.1 #ハニーポット	2021-04-03 06:35:16
 @marwanali2012	شعور جميل انك University of Texas at Austin في جامعة CVE-2019-11581 الحمد لله عثرت على ثغرة تحصل ثغرة في جامعة لط twitter.com/i/web/status/1...	2021-07-28 22:48:29
 @tuhin1729_	(6/n) 9. CVE-2019-11581(SSTI): <a href="http://<JIRA>/secure/ContactAdministrators!default.jspa">http://<JIRA>/secure/ContactAdministrators!default.jspa Try SSTI payload in subject... twitter.com/i/web/status/1...	2021-10-05 06:55:27

← Previous ID

Next ID →

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](#).

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