



CVE-2020-14172

Published on: 07/02/2020 12:00:00 AM UTC

Last Modified on: 05/03/2022 01:59:00 PM UTC

CVE-2020-14172

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

CVSS:31/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:

This issue exists to document that a security improvement in the way that Jira Server and Data Center use velocity templates has been implemented. The way in which velocity templates were used in Atlassian Jira Server and Data Center in affected versions allowed remote attackers to achieve remote code execution via insecure deserialization, if they were able to exploit a server side template injection vulnerability. The affected versions are before version 7.13.0, from version 8.0.0 before 8.5.0, and from version 8.6.0 before version 8.8.1.

CVE-2020-14172 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Atlassian](#) - **Jira Server** version < 7.13.0

Affected Vendor/Software: [Atlassian](#) - **Jira Server** version >= 8.0.0

Affected Vendor/Software: [Atlassian](#) - **Jira Server** version < 8.5.0

Affected Vendor/Software: [Atlassian](#) - **Jira Server** version >= 8.6.0

Affected Vendor/Software: [Atlassian](#) - **Jira Server** version < 8.8.1

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: **7.5 - HIGH**

Access
Vector

Access
Complexity

Authentication

Factor	Complexity	
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[JRASERVER-70940] Template injection in Web Resources Manager - CVE-2020-14172 - Create and track feature requests for Atlassian products.	Permissions Required jira.atlassian.com text/html	 MISC jira.atlassian.com/browse/JRASERVER-70940

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.

There are currently no QIDs associated with this CVE

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 Software Data Center	All	All	All	All
Application	Atlassian	Jira Software Data Center	All	All	All	All

cpe:2.3:a:atlassian:jira:*:*:*:*:*:*:

```
cpe:2.3:a:atlassian:jira:*:*:*:*:*:*:
```

```
cpe:2.3:a:atlassian:jira software data center:*:*:*:*:*.*
```

```
cpe:2.3:a:atlassian:iira software data center:*.:.:.:.:.:.:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← 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](#)