



CVE-2019-20406

Published on: 02/05/2020 12:00:00 AM UTC

Last Modified on: 12/13/2021 04:05:00 PM UTC

CVE-2019-20406

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to write a DLL file in a directory in the global path environmental variable to inject code & escalate their privileges via a DLL hijacking

vulnerability.

CVE-2019-20406 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Atlassian](#) - **Confluence Data Center** version < 7.0.5

Affected Vendor/Software: [Atlassian](#) - **Confluence Data Center** version >= 7.1.0

Affected Vendor/Software: [Atlassian](#) - **Confluence Data Center** version < 7.1.1

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[CONFSERVER-59428] Confluence on Windows was vulnerable to DLL hijacking - CVE-2019-20406 - Create and track feature requests for Atlassian products.	Vendor Advisory jira.atlassian.com text/html	 MISC jira.atlassian.com/browse/CONFSERVER-59428

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	Confluence	All	All	All	All
Application	Atlassian	Confluence	7.1.0	All	All	All
Application	Atlassian	Confluence	All	All	All	All
Application	Atlassian	Confluence	7.1.0	All	All	All
Application	Atlassian	Confluence Server	7.1.0	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:a:atlassian:confluence:*.*.*.*.*.*.*.*.*.*

```
cpe:2.3:a:atlassian:confluence:7.10.*:*:*:*:*:
```

cpe:2.3:a:atlassian:confluence:*:*:*:*:*:

```
cpe:2.3:a:atlassian:confluence:7.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:atlassian:confluence_server:7.1.0:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows:-.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:microsoft:windows:-.*.*.*.*.*.
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#).

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