



Confluence 9.1 (Latest)  
Documentation

/ ... / ... / Confluence Se...

Cloud

Data Center 9.1 ▾

# Security Advisory - 2021-08-25

## Confluence Data Center - CVE- Confluence Server Webwork

### Related content

#### Still need help?

The Atlassian  
Community is here for  
you.

**Ask the  
community**

has been updated since its original

being actively exploited in the wild.  
uld be patched immediately.  
exploitable by unauthenticated users  
ration.  
o clarify how customers can identify  
fluence Cloud

aded to a fixed version, there is no

26084 - Confluence Server Webwork  
ion

t 2021 10AM PDT (Pacific Time, -7

ance Server  
ance Data Center

**Cloud customers are not affected.**



Confluence 9.1 (Latest)  
Documentation

## versions

## versions

## versions

## versions

## versions

## versions

## versions

## versions

## versions

## versions

## versions

## versions

x versions

x versions

x versions

x versions **before** 6.13.23

x versions

x versions

## versions

## versions

## versions

## versions

versions **before** 7.4.11

## versions

## versions

## versions

## versions

## versions

x versions

x versions **before** 7.11.6

x versions **before** 7.12.5

26084



Confluence 9.1 (Latest)  
Documentation

## ibility

erity security vulnerability. Confluence  
**efore version 6.13.23, from version**  
**on 7.5.0 before 7.11.6, and from**  
affected by this vulnerability.

**s are not affected.**

s accessed via  
nain, it is hosted by Atlassian and  
the vulnerability.

**upgraded to versions 6.13.23,**  
**or 7.4.11 are not affected.**

wnloaded and installed any versions  
sions section must upgrade their  
ulnerability. If you are unable to  
ply the workaround detailed below  
rade.

## Confluence Server ection

g actively exploited in the wild.

be patched immediately.

this vulnerability as critical, according to [severity levels](#). The scale allows us to moderate or low.

could evaluate its applicability to your

ists that would allow an arbitrary code on a Confluence Server or

nd Data Center prior to the fixed by this vulnerability.

issue details... STATUS

/ Jacob (SnowyOwl) via the Atlassian

to address this issue:

7.4.11, 7.11.6, 7.12.5, and 7.13.0 which

upgrade to the latest Long Term Support or latest version, see the [Release Notes](#). You can download the [Centre](#).

ion **upgrade to version 7.13.0**

s and **cannot upgrade to 7.13.0** 7.13.23.



Confluence 9.1 (Latest)  
Documentation





Confluence 9.1 (Latest)  
Documentation



and **cannot upgrade to 7.13.0**  
**4.11.**

s and **cannot upgrade to 7.13.0**  
**11.6.**

s and **cannot upgrade to 7.13.0**  
**12.5.**

Confluence immediately, then as  
soon as possible, to  
mitigate the issue by running the  
script that Confluence is hosted on.

[Enter Node running on Linux based](#)

[Enter Node running on Microsoft](#)

If you have received this advisory and you wish to receive  
updates, please visit <https://my.atlassian.com/email> and

if you have any questions regarding this advisory, please raise a  
ticket at <https://my.atlassian.com/>.

Additional security bug fixes will be back  
ported to the versions  
mentioned in the advisory with  
[confluence.atlassian.com/trust/security/bug-fix-policy](https://confluence.atlassian.com/trust/security/bug-fix-policy).  
Future maintenance releases for the versions  
mentioned in the advisory will be released as binary patches.

**These versions are no longer released.**

Confluence Security Advisories include a severity level and a  
CVSS score. The severity level is based on our self-  
assessments and the CVSS score is provided for each specific vulnerability. CVSS



Confluence 9.1 (Latest)  
Documentation

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

ard vulnerability metric. You can also  
VSS at [FIRST.org](#).

cy varies for different products. Please  
icy for details.