



Confluence Data Center

CONFSERVER-91258

DoS (Denial of Service) in Confluence Data Center and Server

▼ Details

Type:

Public Security Vulnerability

Resolution:

Fixed

Priority:

High

Fix Version/s:

8.6.0, 8.5.1, 7.19.14

Affects Version/s:

5.6

Component/s:

None

Labels:

advisory

advisory-to-release

dont-import

failed-to-sanitize

fixed-versions-published

security

CVSS Score:

7.5

CVSS Severity:

High

Vulnerability Source:

Bug Bounty

CVSSv3 Vector:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Vulnerability Classes:

DoS (Denial of Service)

Affected Product(s):

Confluence Data Center, Confluence Server

▼ Description

This High severity DoS (Denial of Service) vulnerability was introduced in version 5.6 of Confluence Data Center and Server. With a CVSS Score of 7.5, this vulnerability allows an unauthenticated attacker to cause a resource to be unavailable for its intended users by temporarily or indefinitely disrupting services of a vulnerable host (Confluence instance) connected to a network, which has no impact on confidentiality, no impact to integrity, high impact to availability, and requires no user interaction.

Affected versions

All Confluence versions from 5.6 onwards apart from 7.19.14 and 8.5.1

Atlassian recommends that Confluence Data Center and Server customers upgrade to the latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions:

- Confluence Data Center and Server 7.19: Upgrade to a release greater than or equal to 7.19.14
- Confluence Data Center and Server 8.5: Upgrade to a release greater than or equal to 8.5.1
- Confluence Data Center and Server 8.6 or above: No need to upgrade, you're already on a patched version


See the release notes <https://confluence.atlassian.com/doc/confluence-release-notes-327.html>.

You can download the latest version of Confluence Data Center and Server from the download center <https://www.atlassian.com/software/confluence/download-archives>.

This vulnerability was reported via our Bug Bounty program.


▼ Issue Links

mentioned in




[Page](#)

Failed to load




[Page](#)

Failed to load




[Page](#)

Failed to load



[Page](#)

Failed to load



[Page](#)

Failed to load


Show 33 more links

(33 mentioned in)

▼ Forms

▼ Activity

Newest first

- ▼  **Tim Eddelbüttel** added a comment - 17/Jan/2024 8:49 AM

Is there a logical reason why the CVE ID was changed from CVE-2023-22512 to CVE-2024-21679 by the Security Metrics Bot?
That CVE ID doesn't exist: <https://nvd.nist.gov/vuln/detail/CVE-2024-21679>

- ▼  **Andy Holt** added a comment - 16/Oct/2023 7:23 AM


@gecon27 the fix to 7.13.x for <https://jira.atlassian.com/browse/CONFSERVER-88221> was issued while 7.13.x wasn't EOL (it had about 2 weeks left 😊)

- ▼  **gecon27** added a comment - 10/Oct/2023 2:44 PM

[Jerome Fath] Also need to know if a bug fix will be released for 7.13.x LTS

[Andy Holt] Unlikely, that version is EOL and out of support.

In another recent vulnerability (refer to <https://jira.atlassian.com/browse/CONFSERVER-88221>), version 7.13x LTS was taken into account and a fix was also provided. How can it be that in this case there is no info whether 7.13.x LTS is affected and is merely considered EOL? Thanks.


- ▼  **Christoph Schramm** added a comment - 05/Oct/2023 8:47 AM

Hello Atlassian Team,

can you clarify on the original vulnerability (DOS vulnerability) in conjunction with your latest security advisory here:
<https://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html>

Does the new announcement supersede this one here and how do they interconnect since the CVE number stays the same? Are versions below 8.x.x also not affected from the vulnerability mentioned in this original issue? Your latest advisory implies that:



-
- ▼  **Dario** added a comment - 03/Oct/2023 12:44 PM - edited

Hi Team,

In my case, yesterday I upgraded our Production environment to **7.19.14** but the **Instance health checks** returns and administration error message saying that this version is affected by this security vulnerability, is it true? if it is so, I would appreciate you change the description of this ticket because 7.19.14 version is affected as well.

Thank you!!

- ▼  **Andy Holt** added a comment - 27/Sep/2023 10:41 AM - edited

> Also need to know if a bug fix will be released for 7.13.x LTS


Unlikely, that version is EOL and out of support.

- ▼  **Jerome Fath** added a comment - 25/Sep/2023 4:15 PM


Also need to know if a bug fix will be released for 7.13.x LTS

▼  [Chris](#) added a comment - 22/Sep/2023 9:43 AM

Why does the internal Confluence-Scan not react to such an issue???

▼  [Rilwan_Ahmed_NC](#) added a comment - 22/Sep/2023 1:44 AM

All Confluence versions from 5.6 onwards apart from 7.19.14 and 8.5.1 are affected.
Ticket description is updated.


▼  [Martha Delgado](#) added a comment - 21/Sep/2023 3:11 PM

Are you guys planning on releasing a new update for version 7.20.3?

[Load more older comments](#)

▼ People

Assignee:

 Unassigned

Reporter:

 Security Metrics Bot 

Votes:

 1 Vote for this issue

Watchers:

 50 Start watching this issue

▼ Dates

Created:

07/Sep/2023 7:28 AM

Updated:

01/Jan/2025 12:00 AM

Resolved:

26/Sep/2023 8:43 AM