Confluence Security Advisory 2022-06-02

Contents

Date	02 Jun 2022
Product	• Confluence Server • Confluence Data Center
Vulnerability	Critical
CVE	CVE-2022-26134
Official link	Confluence Security Advisory 2022-06-02

Confluence Security Advisory - Critical severity unauthenticated remote code execution vulnerability - CVE-2022-26134

Dear customer,

on the 2nd of June 2022 10 PM CEST, Atlassian issued a Security Advisory for Confluence Server & Confluence Data Center. The Cloud versions of the applications as well as other Atlassian products are not affected.

What you need to know

Atlassian has been made aware of current active exploitation of a critical severity unauthenticated remote code execution vulnerability in Confluence Data Center and Server. Further details about the vulnerability are being withheld until a fix is available. There is no proof of concept for this vulnerability so the attack vector is not broadly available to the public.

Atlassian is actively working on a patch for impacted versions and will update the advisory with estimates for completion.

Affected Versions

ⓘ All versions include Confluence Server & Confluence Data Center

What should I do?

Confluence Server & Data Center

You use Confluence Server or Confluence Data Center

Update

Currently there is no fixed version, as soon as Atlassian releases a new version, we will update this page.

Workaround

There are currently no fixed versions of Confluence Server and Confluence Data Center available. In the interim, customers should work with their security team to consider the best course of action. Options to consider include:

- Restricting access to Confluence Server and Data Center instances from the internet.
- Disabling Confluence Server and Data Center instances.

If you are unable to take the above actions implementing a WAF (Web Application Firewall) rule which blocks URLs containing `${` **may reduce your risk**.

This advisory will be updated as fixes become available..

Confluence Cloud

You use Confluence Cloud

✓ You are not affected by this Security Advisory.

No need for action.

bitvoodoo Cloud
You use Confluence Server or Confluence Data Center

Update

Currently there is no fixed version, as soon as Atlassian releases a new version, we will update this page and we will inform affected customers.

LTS Update Package Customers will get an update to the latest LTS release free of charge as soon as possible.

Workaround

> A workaround **has been implemented** to secure instances hosted on the bitvoodoo cloud. We will update the instances as soon as the fixed version is available.

Further Reading

- Volexity - Zero-Day Exploitation of Atlassian Confluence
- CVE-2022-26134
- Confluence Security Advisory 2022-06-02

Support

If you still have questions or concerns regarding this advisory, please contact the bitvoodoo support via support.bitvoodoo.ch.