

Overall rating: Critical



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a critical authentication vulnerability was discovered in Confluence Server and Data Center. All versions of Confluence Data Center and Server are affected by this unexploited vulnerability. There is no impact to confidentiality as an attacker cannot exfiltrate any instance data.

Publicly accessible Confluence Data Center and Server versions as listed below are at critical risk and require immediate attention. See 'What You Need to Do' for detailed instructions.

Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.

Technical Details

Atlassian rates the severity level of this vulnerability as critical (9.1 with the following vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H) per our internal assessment.

This is our assessment, and you should evaluate its applicability to your own IT environment.

Affected Versions

This Improper Authorization vulnerability affects all versions prior to the listed fix versions of Confluence Data Center and Server. Atlassian recommends patching to the fixed LTS version or later.

Product Affected Versions

Confluence Data Center and Server All versions are affected.

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify [VRM](#) with any questions or concerns you may have.

References

- CVE-2023-22518
- [Atlassian Security Bulletin – October 30 2023](#)
- [Atlassian Security Advisories and Bulletins](#)

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: [Cybersecurity Alerts](#)