Broken Access Control Vulnerability in Confluence Server (Oct 2023)

Atlassian is aware of a problem that a few customers have reported. Attackers from outside the company may have used a previously unknown flaw in publicly accessible Confluence Data Center and Server instances to make fake Confluence administrator accounts and get into Confluence instances.

CVE-2023-22515 - Broken Access Control Vulnerability in Confluence Data Center and Server

Still need help?

The Atlassian Community is here for you.

Ask the community

CVE-2023-22515 - Broken Access Control Vulnerability in Confluence Data Center and Server

Summary	CVE-2023-22515 - Broken Access Control Vulnerability in Confluence Data Center and Server
Advisory Release Date	Wed, Oct 4th 2023 06:00 PDT
Products	• Confluence Data Center • Confluence Server
CVE ID	CVE-2023-22515
Related Jira Ticket(s)	• CONFSERVER-92475

Updates

This advisory has been updated since the initial publication.

Changes since initial publication

Summary of Vulnerability

Atlassian has been made aware of an issue reported by a handful of customers where external attackers may have exploited a previously unknown vulnerability in publicly accessible Confluence Data Center and Server instances to create unauthorized Confluence administrator accounts and access Confluence instances.

UPDATE: We have evidence to suggest that a known nation-state actor is actively exploiting CVE-2023-22515 and continue to work closely with our partners and customers to investigate.

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.

CVSS 10: URGENT ACTION REQUIRED

1. Upgrade your instance

2. Conduct comprehensive threat detection

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.

Severity

Atlassian rates the severity level of this vulnerability as Critical CVSS 10, according to the scale published in our Atlassian severity levels. The scale allows us to rank the severity as critical, high, moderate or low. This is our assessment, and you should evaluate its applicability to your own IT environment.

Affected Versions

The Confluence Data Center and Server versions listed below are affected by this vulnerability. Customers using these versions should upgrade your instance as soon as possible.

Versions prior to 8.0.0 are not affected by this vulnerability.

Product	Affected Versions
Confluence Data Center and Confluence Server	• 8.0.0 • 8.0.1 • 8.0.2 • 8.0.3 • 8.0.4 • 8.1.0 • 8.1.1 • 8.1.3 • 8.1.4 • 8.2.0 • 8.2.1 • 8.2.2 • 8.2.3 • 8.3.0 • 8.3.1 • 8.3.2 • 8.4.0 • 8.4.1 • 8.4.2 • 8.5.0 • 8.5.1

What You Need To Do

Immediately patch to a fixed version

Atlassian recommends that you patch each of your affected installations to one of the listed fixed versions (or any later version) below.

Product	Fixed Versions
Confluence Data Center and Server	• 7.19.16 or later • 8.3.4 or later • 8.4.4 or later • 8.5.3 or later • 8.6.1 or later

Apply temporary mitigations if unable to patch

1. **Back up your instance.** (Instructions: https://confluence.atlassian.com/doc/production-backup-strategy-38797389.html)
2. **Remove your instance from the internet until you can patch, if possible.** Instances accessible to the public internet, including those with user authentication, should be restricted from external network access until you can patch.
3. **If you cannot restrict external network access or patch**, apply the following interim measures to mitigate known attack vectors by blocking access on the following endpoints on Confluence instances:
    a. `/json/setup-restore.action`
    b. `/json/setup-restore-local.action`
    c. `/json/setup-restore-progress.action`

4. This is possible at the network layer or by making the following changes to Confluence configuration files.
   On each node, modify `/<confluence-install-dir>/confluence/WEB-INF/web.xml` and add the following block of code (just before the `</web-app>` tag at the end of the file):

```
<security-constraint>
                <web-resource-collection>
                        <url-pattern>/json/setup-restore.action</url-pattern>
                        <url-pattern>/json/setup-restore-local.action</url-pattern>
                        <url-pattern>/json/setup-restore-progress.action</url-pattern>
                        <http-method-omission>*</http-method-omission>
                </web-resource-collection>
        <auth-constraint />
</security-constraint>
```

5. Restart Confluence.

   Note: These mitigation actions are limited and not a replacement for patching your instance; you must patch as soon as possible

For more information, please connect to https://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html