# Multiple Products Security Advisory 2022-07-20

**Contents**



| | |
|---|---|
| **Date** | 20 Jul 2022 |
| **Product** | • Bamboo Server and Data Center<br>• Bitbucket Server and Data Center<br>• Confluence Server and Data Center<br>• Crowd Server and Data Center<br>• Fisheye and Crucible<br>• Jira Server and Data Center<br>• Jira Service Management Server and Data Center |
| **Vulnerability** | Critical |
| **CVE** | CVE-2022-26136, CVE-2022-26137, CVE-2022-26138 |
| **Official link** | • Multiple Products Security Advisory - CVE-2022-26136, CVE-2022-26137<br>• Questions For Confluence App Security Advisory- CVE-2022-26138 |

---

## Multiple Products Security Advisory - CVE-2022-26136, CVE-2022-26137, CVE-2022-26138

Dear customer,

on the 20th of July 2022 10 PM CEST, Atlassian issued two Security Advisories for it's on-premise software products and the Confluence app Questions for Confluence. The Cloud versions of the applications are not affected.

### What you need to know

Atlassian has been made aware of a critical vulnerability in their on-premise software products via Arbitrary Servlet Filter Bypass and Additional Servlet Filter Invocation. Further details about the vulnerability are available in Multiple Products Security Advisory - 2022-07-20. The only current way to secure the applications, is updating to fixed versions.

Additionally Atlassian disclosed a vulnerability in the app Questions for Confluence due to a systemuser with harcoded user credentials. Further details on the vulnerability can be found in Questions For Confluence App Security Advisory - 2022-07-20. Updating Questions for Confluence fixes this vulnerability.

### Affected Versions

| Product | Affected Versions |
|---|---|
| Bamboo Server and Data Center | • Versions < 8.0.9<br>• 8.1.x < 8.1.8<br>• 8.2.x < 8.2.4 |
| Bitbucket Server and Data Center | • Versions < 7.6.16<br>• All versions 7.7.x through 7.16.x<br>• 7.17.x < 7.17.8<br>• All versions 7.18.x<br>• 7.19.x < 7.19.5<br>• 7.20.x < 7.20.2<br>• 7.21.x < 7.21.2<br>• 8.0.0<br>• 8.1.0 |

| | |
|---|---|
| Confluence Server and Data Center | • Versions < 7.4.17<br>• All versions 7.5.x through 7.12.x<br>• 7.13.x < 7.13.7<br>• 7.14.x < 7.14.3<br>• 7.15.x < 7.15.2<br>• 7.16.x < 7.16.4<br>• 7.17.x < 7.17.4<br>• 7.18.0 |
| Crowd Server and Data Center | • Versions < 4.3.8<br>• 4.4.x < 4.4.2<br>• 5.0.0 |
| Crucible | • Versions < 4.8.10 |
| Fisheye | • Versions < 4.8.10 |
| Jira Server and Data Center | • Versions < 8.13.22<br>• All versions 8.14.x through 8.19.x<br>• 8.20.x < 8.20.10<br>• All versions 8.21.x<br>• 8.22.x < 8.22.4 |
| Jira Service Management Server and Data Center | • Versions < 4.13.22<br>• All versions 4.14.x through 4.19.x<br>• 4.20.x < 4.20.10<br>• All versions 4.21.x<br>• 4.22.x < 4.22.4 |
| Questions for Confluence | • Any versions 2.7.x and 3.0.x may be affected, refer to What should I do? |

## Fixed Versions



bitvoodoo recommends using the **latest LTS releases** of Jira, Confluence, and Bitbucket.

| Product | Fixed Versions |
|---|---|
| Bamboo Server and Data Center | • >= 8.0.9<br>• >= 8.1.8<br>• >= 8.2.4<br>• >= 9.0.0 |
| Bitbucket Server and Data Center | • >= 7.6.16 (LTS)<br>• >= 7.17.8 (LTS)<br>• >= 7.19.5<br>• >= 7.20.2<br>• **>= 7.21.2 (LTS)**<br>• >= 8.0.1<br>• >= 8.1.1<br>• >= 8.2.0 |

| | |
|---|---|
| Confluence Server and Data Center | • >= 7.4.17 (LTS)<br>• **>= 7.13.7 (LTS)**<br>• >= 7.14.3<br>• >= 7.15.2<br>• >= 7.16.4<br>• >= 7.17.4<br>• >= 7.18.1<br>• >= 7.19.0 |
| Crowd Server and Data Center | • >= 4.3.8<br>• >= 4.4.2<br>• >= 5.0.1 |
| Crucible | • >= 4.8.10 |
| Fisheye | • >= 4.8.10 |
| Jira Server and Data Center | • >= 8.13.22 (LTS)<br>• **>= 8.20.10 (LTS)**<br>• >= 8.22.6<br>• >= 9.0.0 |
| Jira Service Management Server and Data Center | • >= 4.13.22 (LTS)<br>• **>= 4.20.10 (LTS)**<br>• >= 4.22.6<br>• >= 5.0.0 |

## What should I do? - On-Premise Products

**Server & Data Center**
**You use the Server or Data Center variant of any Atlassian application in a version listed in Affected Versions.**

### Update

Update to a version listed in Fixed Versions.

⚠ bitvoodoo recommends using the latest LTS releases of Jira, Confluence and Bitbucket.

### Workaround

There are currently no workarounds.

**Cloud**
**You use Jira, Confluence or Bitbucket Cloud.**

✓ You are not affected by this Security Advisory.

***No need for action.***

**bitvoodoo Cloud**
**You use Jira, Confluence or Bitbucket Server or Data Center hosted with bitvoodoo.**

### Update

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

bitvoodoo Cloud customers who do not have an LTS update package will be contacted by bitvoodoo in the coming days for coordination for an update.

### Workaround

There are currently no workarounds.

## What should I do? - Questions For Confluence App

**Server & Data Center**

**You use the app Questions for Confluence in Confluence Server or Data Center.**

### Determine If You Are Affected

Determine if you are affected by searching for the `disabledsystemuser` user account. If this account does not show up in the list of active users, the Confluence instance is not affected.

### Update the App

Update the Questions for Confluence app to a fixed version:

- 2.7.x >= 2.7.38 (compatible with Confluence 6.13.18 through 7.16.2)
- Versions >= 3.0.5 (compatible with Confluence 7.16.3 and later)

### Workaround

Search for the `disabledsystemuser` user account and either disable it or delete it. For instructions on how to disable or delete an account (including an explanation of the differences between the two options), refer to:

- Delete or Disable Users | Atlassian Documentation

**Cloud**

**You use Confluence Cloud.**

You are not affected by this Security Advisory.

***No need for action.***

**bitvoodoo Cloud**

**You use the app Questions for Confluence in Confluence Server or Data Center hosted with bitvoodoo.**

bitvoodoo already updated Questions for Confluence in all Confluence installation hosted with bitvoodoo.

***No need for action.***

# Further Reading

- CVE-2022-26136
- CVE-2022-26137
- CVE-2022-26138
- Multiple Products Security Advisory - 2022-07-20
- Questions For Confluence App Security Advisory - 2022-07-20

## Support

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