Jira Server and Data Center Security Advisory - 2022-04-20

Contents

Date	20 Apr 2022
Product	Jira Core Server Jira Software Server Jira Software Data Center Jira Service Management Server Jira Service Management Data Center
Vulnerability	Critical
CVE	CVE-2022-0540
Official link	Jira Security Advisory 2022-04-20

Jira Server and Data Center Security Advisory - Authentication Bypass in Seraph - CVE-2022-0540

Dear customer,

on the 20th April 2022 22:00 PM UST, Atlassian issued a Security Advisory for Jira Server & Data Center. The Cloud versions of the applications as well as other Atlassian products are not affected.

What you need to know

Atlassian discovered a security vulnerability regarding an authentication bypass in the web authentication framework, Jira Seraph. Although the vulnerability is in the core of Jira, it affects first and third party apps that specify the use of some specific roles. A remote, unauthenticated attacker could exploit this by requesting a specially crafted HTTP request to bypass authentication and authorization requirements in WebWork actions using an affected configuration.

An app is only affected by CVE-2022-0540 when both of the following conditions are true:

- It’s installed in one of the affected Jira or Jira Service Management versions listed above.
- It’s using a configuration vulnerable to CVE-2022-0540.

Affected Versions

> All versions include Jira Server & Data Center

Jira Core, Jira Software

- All versions before 8.13.18
- 8.14.x
- 8.15.x
- 8.16.x
- 8.17.x
- 8.18.x
- 8.19.x
- 8.20.x before 8.20.6
- 8.21.x

Jira Service Management

- All versions before 4.13.18
- 4.14.x
- 4.15.x

- 4.16.x
- 4.17.x
- 4.18.x
- 4.19.x
- 4.20.x before 4.20.6
- 4.21.x

Apps

- Insight - Asset Management
    - Versions 8.x and earlier are available from the Atlassian Marketplace
    - Versions 9.x are bundled with Jira Service Management Server and Data Center 4.15.0 and later
- Mobile Plugin for Jira
    - Bundled with Jira Server, Jira Software Server and Data Center 8.0.0 and later
    - Bundled with Jira Service Management Server and Data Center 4.0.0 and later
- Marketplace Apps
    - A list with affected Apps can be found on Jira Security Advisory 2022-04-20 under "Determining which apps are affected"

Fixed Versions

Jira Core, Jira Software

- 8.13.18
- 8.20.6
- 8.22.0

Jira Service Management

- 4.13.18
- 4.20.6
- 4.22.0

You can download the latest versions from the download pages for Jira Core or Jira Software or Jira Service Management.

Please Note: These are the first versions that include the fix for CVE-2022-0540. More current bug fix releases are available for the releases listed above. Atlassian recommends upgrading to the most current bug fix version.

What should I do?

Jira Server & Data Center

You use Jira Server or Data Center

Update

Installing a fixed version of Jira or Jira Service Management is the best way to remediate CVE-2022-0540. Once a fixed version has been installed, all apps in your instance are protected against CVE-2022-0540 and no further action is required.

Update Jira to one of the listed Fixed Versions.

Workaround

If you’re unable to install a fixed version of Jira or Jira Service Management and you’re using any affected apps, refer to the list of affected apps in the section "A*ffected Versions"* above. If non-affected versions of those apps are available, update any affected apps.

- If updates with fix are available for Marketplace apps, ***update*** the respective apps.
- If no version with fix is available, ***disable*** the respective apps.

DO NOT disable Insight - Asset Management on the following versions of Jira Service Management:

- 4.19.x
- 4.20.x < 4.20.3

In these versions of Jira Service Management, disabling **Insight - Asset Management** causes all of Jira Service Management to be disabled.

For more information on how to disable the **Insight - Asset Management** app, refer to this Jira KB article.

Jira Cloud
You use Jira Software, Jira Service Management or Jira Work Management Cloud

> ✓ You are not affected by this Security Advisory.

No need for action.

bitvoodoo Cloud
Your Jira Server or Data Center is hosted with bitvoodoo

Update

Installing a fixed version of Jira or Jira Service Management is the best way to remediate CVE-2022-0540. Once a fixed version has been installed, all apps in your instance are protected against CVE-2022-0540, and no further action is required.

We can offer you an update to a fixed version at short notice.

- If you have a **"LTS Release" Update Package**, we will implement an update free of charge.
- **Else, ask bitvoodoo as soon as possible to update Jira to one of the listed Fixed Versions.**

Workaround

bitvoodoo will help you determine which apps are affected and will implement workarounds where possible.

Further Reading

- FAQ for CVE-2022-0540
- CVE-2021-0540

Support

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