Jira Service Management Security Advisory - 2021-10-20

Date	20 Oct 2021
Product	• Insight - Asset Management app • Jira Service Management Data Center • Jira Service Management Cloud customers are not affected.
Vulnerability	Critical
Official link	Link

Dear customer,

Atlassian has published on Wednesday a critical security advisory pointing to a security vulnerability in "Insight - Asset Management App" respectively "Jira Service Management Data Center".

Affected versions

Insight - Asset Management version:

- All 5.x versions
- All 6.x versions
- All 7.x versions
- All 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, 8.5.x, 8.6.x, 8.7.x, 8.8.x versions
- All 8.9.x versions before 8.9.3

Jira Service Management both Server and Data Center version:

- All 4.15.x versions (Insight v. 9.0.x bundled)
- All 4.16.x versions (Insight v. 9.0.x bundled)
- All 4.17.x versions (Insight v. 9.0.x bundled)
- All 4.18.x versions (Insight v. 9.0.x bundled)
- All 4.19.x versions (Insight v. 9.1.0 bundled)

Fixed versions - Insight - Asset Management Marketplace App

8.9.3

Fixed versions - Jira Service Management

4.20.0 (Insight v. 9.1.2 bundled)

CVE ID(s)

CVE-2018-10054

Summary of Vulnerability

This advisory discloses a **critical severity** security vulnerability in versions of the **Insight - Asset Management** app prior to 8.9.3. This app is bundled with Jira Service Management (known as Jira Service Desk prior to 4.14) from version 4.15.0 onwards. All versions of Jira Service Management (Server/Data Center) >= 4.15.0 and < 4.20 are impacted. Affected versions of the Insight - Asset Management app and Jira Service Management are listed in the table above (see **Affected Versions**)

> ⓘ Jira Service Management Cloud customers are not impacted by this.

> ⓘ Customers who have upgraded to Jira Service Management version 4.20.0 and Insight - Asset Management app version 8.9.3 or above are not affected.

⚠ **If you've downloaded and installed any versions listed in the Affected versions section, you must upgrade your installations to fix this vulnerability. If you are unable to upgrade immediately, apply the workaround detailed below while you plan your upgrade.**

CVE-2018-10054 - RCE in Insight - Asset Management impacting Jira Service Management Data Center

Severity

Atlassian rates the severity level of this vulnerability as **critical**, 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.

Description

Insight - Asset Management has a feature to import data from several databases (DBs). One of these DBs, the H2 DB, has a native function in its library which an attacker can use to run code on the server (remote code execution a.k.a. RCE). The H2 DB is bundled with Jira to help speed up the setup of Jira test environments.

The combination of the DB import feature introduced by Insight - Asset Management with the existing Jira H2 DB library exposed this vulnerability. The vulnerability exists whether or not the import configuration was saved and even if H2 was never used as a targeted DB. Accessing this vulnerability requires the following:

- The user must be an authenticated Jira user **AND**

Either of the following privileges within Insight - Asset Management:

- user or group permission to “Insight administrator”
- user or group permission to “Object Schema Manager”

ⓘ Jira Service Management Data Center versions 4.15.0 and greater have Insight - Asset Management already bundled.

ⓘ Jira Core (Server/DC), Jira Software (Server/DC), and Jira Service Management (Server) instances that use H2 DB **without** Insight - Asset Management installed from the Marketplace aren't affected by this vulnerability.

This issue can be tracked here: blocked URLJSDSERVER-8716 - Jira Service Management / Insight Asset Management vulnerable to RCE Security

Fix

We have taken the following steps to address this issue:

1. Released versions 4.20.0 of Jira Service Management and 8.9.3 of the Insight - Asset Management app, which disables the import feature from making a connection to any H2 DB.

What you need to do

Atlassian recommends that you upgrade to the latest fix version but if you can’t, you should follow the mitigation steps. For a full description of the latest version of Jira Service Management and Insight - Asset Management, see the Jira Service Management release notes.

Upgrade

Jira Service Management

For Jira Service Management (Server/Data Center) versions 4.15.0 and greater, upgrade to 4.20.0 by downloading it from our software downloads page. Note that for these versions, you can't only upgrade the Insight app from the Marketplace as it's bundled with Jira Service Management Data Center.

Insight - Asset Management app

For:

- Jira Service Management (Server/Data Center) versions prior to version 4.15.0,
- Jira Core (Server/Data Center),
- Jira Software (Server/Data Center),

upgrade the Insight - Asset Management app to version 8.9.3 (which disables the connection to any H2 DB) by downloading it from the Atlassian Marketplace.

Consider compatibility with Jira as well. The fix version (8.9.3) of the app is compatible with:

App version	Application compatibility
8.9.3	Server • Jira Core Server 8.12.0 - 8.20 • Jira Software Server 8.12.0 - 8.20 • Jira Service Management Server 4.12 - 4.20 Data Center • Jira Core Data Center 8.12.0 - 8.20 • Jira Software Data Center 8.12.0 - 8.20 • Jira Service Desk Data Center 4.12 - 4.14

If you're running any other version, you must first upgrade to a version that is compatible with the 8.9.3 app (read our security bug fix policy for details). For example, if you're running Jira version 8.7.2 with the Insight - Asset Management app version 8.4.1, you must first upgrade to Jira version 8.12.0 or greater to be able to install the Insight - Asset Management app version 8.9.3. If you can’t upgrade immediately, follow the mitigation steps below.

Mitigation

If you’re unable to upgrade to the latest version immediately, then as a **temporary workaround**, you can mitigate the issue by deleting the H2 JAR file that comes with Jira installation.

> The mitigation steps below will prevent any instances currently using H2 from starting up. You must migrate from the H2 database to any of the other supported database types prior to implementing the mitigation steps in order to keep using the instance.
>
> **H2 databases have never been supported in production environments.**
>
> For guidance on how to migrate databases see Switching databases | Administering Jira applications Data Center and Server 8.19 | Atlassian Documentation.

To remove the H2 JAR file:

1. Shut down Jira
2. Go to `<Jira-Installation-Directory>/atlassian-jira/WEB-INF/lib/`
3. Locate the `h2-1.4.XYZ.jar` file and delete it (where “XYZ” is a placeholder for the version of the file, e.g. `h2-1.4.200.jar`)
4. Start Jira again

> In a Data Center environment, a rolling restart of the nodes is sufficient after deleting the JAR.