

Security Vulnerability — You can access restricted project data with the Connect operation

JIRA SERVER

JIRA CLOUD

In this version of Exalate, you can access data from an access restricted project with the [Connect](#) operation.

In this Section

[How the Vulnerability Works](#)
[Workarounds](#)
[See also](#)

How the Vulnerability Works

Let's assume that **john.doe** is a regular user with no admin access to Jira.

The Jira has following setup

- An Exalate connection.
- A Jira project where **john.doe** has access to issues. Let's call it **Project A**.
- A Jira project where **john.doe** has no access to issues. Let's call it **Project B**.

With these permissions, **john.doe** can create an issue in **Project A**, and connect it to an issue from **Project B**, even though he has no access to **Project B**.

He can do this as follows:

1. Connect the issue manually:
 - In Jira Server, navigate to **More Connect**.
 - In Jira Cloud, navigate to **Exalate Connect issues**.
2. Select the connection in the **Connection** dropdown.

The screenshot shows a modal dialog titled "Connect to remote issue". It features a "Connection" dropdown menu with the placeholder text "Select a connection name" and a "Remote issue key" text input field. At the bottom right, there are "Submit" and "Cancel" buttons. On the right side of the dialog, there is a vertical sidebar with labels: "Assignee:", "Reporter:", "Votes:", "Watchers:", "Created:", "Updated:", and "Exalate".

3. Enter the issue key of the restricted issue in the **Remote issue key**.
4. Press **Submit**.

From now on, this issue in **Project A** (the public project) will receive data from the private issue of **Project B** (the restricted project).

Workarounds

Until we resolve this, we recommend the following workarounds:

1. Ensure that the Exalate proxy user has no access to restricted projects.
2. Disable the Connect operation. This can be done by unchecking **Show Exalate and Connect actions** in the [General Settings](#).



Advanced users would be able to perform a Connect operation through a REST API call. Because of this, we recommend making sure that the proxy user has no access to disabling the Connect operation.

See also

[Connect Operation](#)

[Proxy user](#)

[Local connection](#)

[General Settings](#)