Security Vulnerability — You can Access Restricted Project Data with the Connect Operation

In this version of Exalate, you can access data from a restricted project with the Connect operation.

How the Vulnerability Works

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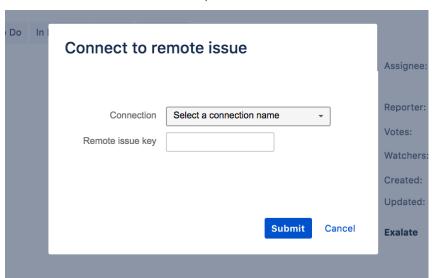
Jira has the following setup

- 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.

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

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.

   > **Note**: 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 disable the Connect operation.

3. For scripted connections - in the outgoing sync script, ensure that no secure information is sent

```
// put this in the first lines of the outgoing sync script to ensure that nothing of the secret project is being sent out.
if (issue.project.name == "Secret") {
  return
}
```