# Redmine - Patch #23376

## Downloading of attachments with MIME type text/javascript fails

2016-07-19 17:51 - Holger Just

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Jean-Philippe Lang | **% Done:** | 0% |
| **Category:** | Attachments | **Estimated time:** | 0.00 hour |
| **Target version:** | 3.3.1 | | |

**Description**

Right now, if you try to download an attachment with content type text/javascript with Redmine 3, it will be blocked by the CSRF protection of Rails. The user-visible response will be an HTTP 422.

This is because Rails thinks that these attachments are dynamic JavaScript resources and thus have to fall under the same origin policy. Unless the request is an AJAX (hxr) request, the downloads are blocked by the verify_same_origin_request after filter which is part of the CSRF protection. This behavior was added to Rails 4.1 in https://github.com/rails/rails/pull/13345.

The attached patch excludes the AttachmentController#download action from this protection, allowing to download javascript attachments. This change won't cause an XSS vulnerability in Redmine but technically allows a specific attack of external sites:

- Given the attacker (Mallory) knows the attachment download URL of a javascript attachment.
- Given a user (Alice) is logged in to Redmine in their browser with permission to download the attachment.
- If Mallory can trick Alice into visiting a Website which includes a <script> tag referencing the attachment, Alice's browser will download and execute the JS file as a classic CSRF. An attacker controlling the website might then be able to extract data from the executed script.

Unfortunately, there is not really a way around this if we want to support JS attachments (with the correct mime type) at all. Since JS attachments typically don't contain secrets though, this is probably acceptable. With the attached patch, we just fall back to the pre-Rails 4.1 behavior for attachments.

Note that this issue is not directly reproducible on Chrome as uploaded JS files are sent with application/javascript instead of text/javascript which doesn't trigger the rule in Rails.

The patch is only relevant for Redmine versions using Rails 4.1 or newer, i.e. Redmine 3. The issue was detected in Planio and fixed by our staff.

### Associated revisions

**Revision 15856 - 2016-10-01 11:24 - Jean-Philippe Lang**

Allow to download javascript attachments again (#23376).

Patch by Holger Just.

**Revision 15877 - 2016-10-02 12:22 - Jean-Philippe Lang**

Merged r15856 (#23376).

### History

**#1 - 2016-07-30 05:00 - Go MAEDA**

*- Target version set to Candidate for next minor release*

**#2 - 2016-09-05 23:55 - Go MAEDA**

*- Target version changed from Candidate for next minor release to 3.3.1*

I reproduced the problem by updating attachments table directly.
Setting target version to 3.3.1.

**#3 - 2016-10-01 11:26 - Jean-Philippe Lang**

*- Status changed from New to Resolved*

*- Assignee set to Jean-Philippe Lang*

Patch committed, thanks. Test changed to use its own attachment instead of a fixture.

#### #4 - 2016-10-02 12:22 - Jean-Philippe Lang

*- Status changed from Resolved to Closed*

### Files

| | | | |
|---|---|---|---|
| 0001-Allow-to-download-javascript-attachments-again.patch | 3.53 KB | 2016-07-19 | Holger Just |