Redmine - Feature #35001
Disable API authentication with username and password when two-factor authentication is enabled for the user

2021-04-02 05:18 - Go MAEDA

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

In Redmine 4.2, two-factor authentication has been introduced.

When two-factor authentication is enabled, it becomes difficult for an attacker to log in to Redmine even if he knows the username and password.

However, API authentication is not covered by two-factor authentication. Currently, there are three methods of API authentication:

1. send the user's API key via X-Redmine-API-Key header
2. basic authentication with the user's API key (username is the API key and password is a random string)
3. basic authentication with user name and password

If you have two-factor authentication enabled, I think the third method will be problematic. This is because even though the web UI can prevent an attacker from logging in with an illegally obtained username and password, they can still use that username and password to access the data via the API.

To address this risk, I suggest disabling basic authentication with username and password for users who have two-factor authentication enabled.

Related issues:

Related to Redmine - Feature # 1237: Add support for two-factor authentication	**Closed**	**2008-05-14**

History

#1 - 2021-04-02 05:26 - Go MAEDA

The following code is a sample implementation.

```
diff --git a/app/controllers/application_controller.rb b/app/controllers/application_controller.rb
index b5644e89d..ec64e74cf 100644
--- a/app/controllers/application_controller.rb
+++ b/app/controllers/application_controller.rb
@@ -129,7 +129,11 @@ class ApplicationController < ActionController::Base
     elsif /\ABasic /i.match?(request.authorization.to_s)
       # HTTP Basic, either username/password or API key/random
       authenticate_with_http_basic do |username, password|
-        user = User.try_to_login(username, password) || User.find_by_api_key(username)
+        user = User.try_to_login(username, password)
+        # Don't allow using username/password when two-factor auth is active
+        user = nil if user&.twofa_active?
+
+        user ||= User.find_by_api_key(username)
       end
```

```
if user && user.must_change_password?
  render_error :message => 'You must change your password', :status => 403
```

#2 - 2021-06-22 20:07 - Marius BALTEANU

- Related to Feature #1237: Add support for two-factor authentication added