

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

2022/05/09 19:12 - Admin Redmine

ステータス:	Closed	開始日:	2022/05/09
優先度:	通常	期日:	
担当者:		進捗率:	0%
カテゴリ:	Accounts / authentication_7	予定工数:	0.00時間
対象バージョン:	5.0.0_155	作業時間:	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/35001	status_id:	5
category_id:	7	tracker_id:	2
version_id:	155	plus1:	0
issue_org_id:	35001	affected_version:	
author_id:	332	closed_on:	
assigned_to_id:	107353	affected_version_id:	
comments:	8		

説明

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.

journals

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 /\/Basic\/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&.two_fa_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
```

Attaching a patch.

Setting the target version to 5.0.0.

Patch committed, thanks!

related_issues

relates,Closed,1237,Add support for two-factor authentication

履歴

#1 - 2022/05/10 16:59 - Admin Redmine

- カテゴリ を Accounts / authentication_7 にセット

- 対象バージョン を 5.0.0_155 にセット