CVE-2020-14380: Users can gain elevated rights when logging in with SSO accounts

Description
User that are authenticated via keycloak/RH SSO can claim the rights of already existing local users

Version-Release number of selected component (if applicable):
6.7.2+

Steps to Reproduce:
1. Create user sectest (local on Satellite) with Sat admin rights and password redhat (Authorized by: INTERNAL)
2. Create user sectest (on RH SSO) with different password
3. Login to Satellite with the SSO user

Actual results:
The user sectest from SSO has full admin rights on the Satellite

Expected results:
Local users on Satellite with authorization source INTERNAL should not be able to login via SSO

Additional info:

Scenario:
- local admin user exists, example "admin"
- SSO admin creates user with the same name in SSO
- The SSO admin user can login to Satellite and has admin rights
- this is even worse as the users in SSO may be federated from other ldap or ADS sources and the Satellite admins have no idea the same users exist in other directories'

Associated revisions
Revision d4449890 - 09/03/2020 12:43 PM - Rahul Bajaj
Fixes #30739 - User must login with the assigned auth source

History
#1 - 08/30/2020 07:49 AM - Tomer Brisker
- Private changed from No to Yes
- Subject changed from Users can gain elevated rights when logging in with SSO accounts to Users can gain elevated rights when logging in with SSO accounts
Patch/fix for review:

diff --git a/app/models/user.rb b/app/models/user.rb
index bacb31f..c75724b 100644
--- a/app/models/user.rb
+++ b/app/models/user.rb
@@ -325,6 +325,9 @@ class User < ApplicationRecord
  new_usergroups += auth_source.external_usergroups.includes(:usergroup).where(:name => external_groups).map(&:usergroup)
  user.update(Hash[attrs.select { |k, v| v.present? }])
  user.usergroups = new_usergroups.uniq
+else
+  logger.info "Failed to create external User: Username '#{attrs[:login]}' already exists"
+  user = nil
+end

user

diff --git a/test/models/user_test.rb b/test/models/user_test.rb
index a72c492..f8adcff 100644
--- a/test/models/user_test.rb
+++ b/test/models/user_test.rb
@@ -718,11 +718,11 @@ class UserTest < ActiveSupport::TestCase
  not_existing_auth_source = 'new_external_source'

-context "internal or not existing AuthSource" do
-  test 'existing user' do
+  test 'existing user without auth source specified' do
+    user = User.find_or_create_external_user({login => existing_user.login}, @apache_source.name)
+    assert user.nil?
+end
+
end
end

test 'existing user of different authsource' do
+  existing_source = AuthSourceExternal.where(:name => 'existing_source').first_or_create
+  existing_user = FactoryBot.create(user, :auth_source => existing_source)
+  user = User.find_or_create_external_user({:login => existing_user.login}, @apache_source.name)
+  assert user.nil?
+end

test "not existing with attributes" do
  created_user = User.find_or_create_external_user({:login => not_existing_user_login,
#4 - 09/01/2020 07:58 AM - Tomer Brisker
- Private changed from Yes to No
- Subject changed from Users can gain elevated rights when logging in with SSO accounts to CVE-2020-14380: Users can gain elevated rights when logging in with SSO accounts

#5 - 09/01/2020 12:57 PM - The Foreman Bot
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/7953 added

#6 - 09/02/2020 08:55 AM - Tomer Brisker
- Target version set to 2.1.3

#7 - 09/03/2020 12:43 PM - The Foreman Bot
- Fixed in Releases 2.3.0 added

#8 - 09/03/2020 12:49 PM - Tomer Brisker
- Fixed in Releases 2.0.3, 2.1.3, 2.2.0 added
- Fixed in Releases deleted (2.3.0)

#9 - 09/03/2020 01:01 PM - Rahul Bajaj
- Status changed from Ready For Testing to Closed

Applied in changeset foremanid4449890acbd24f7a42b0bd8c03cc65339d819b7.

#10 - 09/10/2020 05:12 AM - The Foreman Bot
- Pull request https://github.com/theforeman/foreman/pull/7975 added