CVE-2019-14825: Registry credentials are captured in plain text in dynflow task during repository discovery

07/31/2019 03:14 PM - Justin Sherrill

Status: Closed
Priority: Normal
Assignee: Justin Sherrill
Category: Repositories
Target version: Katello 3.12.2

Pull request: https://github.com/Katello/katello/pull/825
3,
https://github.com/Katello/katello/pull/824
4

Triaged: Yes
Bugzilla link: 1730668

Description
Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1730668

Description of problem:
Observed in the server running on-
Always

Steps to Reproduce:
1. Login to Satellite WebUI
2. Content> Products> Repo Discovery
3. Select 'Container Images' for 'Repository Type'
4. Select 'Red Hat registry' or 'custom' for 'Registry to Discover'
5. Enter registry username and password
6. click on 'Discover'
7. Check the relevant task on the tasks page and verify the dynflow console, the action Actions::Katello::Repository::Discover shows
the input parameters which contains upstream_password in plain text.

Actual results:
Password is visible in plain text, e.g.-

url: registry.access.redhat.com
content_type: docker
upstream_username: admin
upstream_password: test

Expected results:
upstream_password should be encrypted

Related issues:
Related to Katello - Feature #18253: repo search for docker image repos using...
Closed 01/26/2017

Associated revisions
Revision bc9fa139 - 08/01/2019 02:46 PM - Justin Sherrill
Fixes #27485 - encrypt discovery password within task

Revision 33248423 - 08/05/2019 11:30 PM - Chris Roberts
Refs #27485 - Clear proxy settings for tests

History
#1 - 07/31/2019 03:21 PM - The Foreman Bot
- Assignee set to Justin Sherrill
- Status changed from New to Ready For Testing
- Pull request https://github.com/Katello/katello/pull/8244 added

#2 - 07/31/2019 05:36 PM - Justin Sherrill
- Triaged changed from No to Yes
- Target version set to Katello 3.12.2
- Subject changed from Registry credentials are captured in plain text in dynflow task during repository discovery to Registry credentials are captured in plain text in dynflow task during repository discovery

#3 - 08/01/2019 02:46 PM - The Foreman Bot
- Fixed in Releases Katello 3.14.0 added

#4 - 08/01/2019 03:02 PM - Justin Sherrill
- Status changed from Ready For Testing to Closed

Applied in changeset katello|bc9fa1391334a165b22e89a3a3e2e5142b21dddb.

#5 - 08/05/2019 08:03 PM - The Foreman Bot
- Pull request https://github.com/Katello/katello/pull/8253 added

#6 - 09/12/2019 09:40 AM - Tomer Brisker
- Subject changed from Registry credentials are captured in plain text in dynflow task during repository discovery to CVE-2019-14825: Registry credentials are captured in plain text in dynflow task during repository discovery

#7 - 12/31/2019 01:31 PM - Tomer Brisker
- Related to Feature #18253: repo search for docker image repos using the results of docker search added