AzureRM - Bug #31938
CVE-2021-3413 Azure compute resource secret_key leak to authenticated users
02/22/2021 03:56 PM - Evgeni Golov

Status: Closed
Priority: Normal
Assignee: Evgeni Golov
Category: General Plugin Issues
Target version: 2.2.0
Difficulty: 
Pull request: https://github.com/theforeman/foreman_azure_rm/pull/103
Triaged: Yes
Bugzilla link: 1928786
Found in Releases: 

Description
Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1928786

authenticated users can acquire credentials of compute resources

1. prerequisites
   - user with the view_compute_resources permission (e.g. like granted by the "Viewers" role)
   - Azure RM compute resource configured

1. tested environment

Foreman 2.1 with Azure RM compute resource

1. leak

When the `/api/compute_resources/:id/` API endpoint is accessed, it contains the secret_key of the Azure RM user (also the tenant, app_ident etc data that is required to connect, but I think secret_key is the only secret here).

Version-Release number of selected component (if applicable):
2.1 with Azure RM plugin

How reproducible:
100%

Steps to Reproduce:
1. access /api/compute_resources/:id/
2. see credentials in the JSON

Actual results:
JSON contains "secret_key":"THE_KEY"

Expected results:
JSON doesn't contain the "secret_key" entry

Additional info:

Associated revisions
Revision cddff90e - 03/01/2021 05:59 AM - Evgeni Golov
Fixes #31938 - CVE-2021-3413 Azure compute secret_key leak

History
#1 - 02/22/2021 03:59 PM - The Foreman Bot
- Assignee set to Evgeni Golov

03/03/2022
- Pull request https://github.com/theforeman/foreman_azure_rm/pull/103 added

#2 - 03/01/2021 06:01 AM - Evgeni Golov
- Status changed from New to Closed

Applied in changeset foreman_azure_rm|ccdff90e9c2497a53114c686571b6bad911f1a6bd.

#3 - 03/18/2021 01:59 PM - Chris Roberts
- Triaged changed from No to Yes
- Target version set to 2.2.0
- Category set to General Plugin Issues
- Subject changed from CVE-2021-3413 Azure compute resource secret_key leak to authenticated users to CVE-2021-3413 Azure compute resource secret_key leak to authenticated users

#4 - 03/18/2021 02:00 PM - Chris Roberts
- Fixed in Releases 2.2.0 added

03/03/2022
2/2