

[New issue](#)[Jump to bottom](#)

Do not put the subscription-manager password onto the command line. #492

[Merged](#) bocekm merged 11 commits into `oamg:main` from `abadger:fix-sub-mgr-cli-call` on May 27

Conversation 72 Commits 11 Checks 16 Files changed 13



abadger commented on May 10 • edited ▾

Member

Passing values on the command line is insecure. With this change, the rhsm password is passed interactively to subscription-manager instead of being passed on the commandline when we shell out to it.

The structure of this change deserves a bit of description. Previously, we called one function to assemble all of the information needed to invoke subscription-manager and then returned that as a string that could be run as a command line. We called a second function with that string to actually run the command.

To send the password interactively, we need to stop adding the password to the string of command line arguments but it still makes sense to keep the code that figures out the password together with the code which finds the other command line args. So it makes sense to keep a single function to do that but return the password and other args separately.

We could use a dict, a class, or a tuple as the return value from the function. That doesn't feel too ugly. But then we need to pass that structure into the function which takes care of invoking subscription-manager on the command line and that *does* feel ugly. That function would have to care about the structure of the data we pass in (If a tuple, what is the order? If a dict, what are the field names?, etc). To take care of this, we can make the data structure that we return from assembling the data a class and the function which calls subscription-manager a method of that class because it's quite natural for a method to have knowledge of what attributes the class contains.

Hmm... but now that we have a class with behaviours (methods), it starts to feel like we could do some more things. A function that fills in the values of a class, validates that the data is proper, and then returns an instance of that class is really a constructor, right? So it makes sense to move the function which assembles the data and returns the class a constructor. But that particular function isn't very generic: it uses knowledge of our global `toolopts.tool_opts` to populate the class. So let's write a simple `init()` that takes all of the values needed as separate parameters and then create an alternative constructor (an `@classmethod` which returns an instance of the class) which gets the data from a `ToolOpt`, and then calls `init()` with those values and returns the resulting class.

Okay, things are much cleaner now, but there's one more thing that we can do. We now have a class that has a constructor to read in data and a single method that we can call to return some results. What do we call an object that can be called to return a result? A function or more generically, in python, a `Callable`. We can turn this class into a callable by renaming the method which actually invokes `subscription-manager call()`.

What we have at the end of all this is a way to create a function which knows about the settings in `tool_opts` which we can then call to perform our `subscription-manager` needs::

```
registration_command = RegistrationCommand.from_tool_opts()
return_code = registration_command()
```

OAMG-6551 #done convert2rhel now passes the rhsm password to subscription-manager securely.

- Modify the hiding of secret to hide both `--password SECRET` and `--password=SECRET`. Currently we only use it with passwords that we are passing in the second form (to `subscription-manager`) but catching both will future proof us in case we use this function for more things in the future. (Eric Gustavsson)
 - Note: using generator expressions was tried here but found that they only bind the variable being iterated over at definition time, the rest of the variables are bound when the generator is used. This means that constructing a set of generators in a loop doesn't really work as the loop variables that you use in the generator will have a different value by the time you're done.

So a nested for loop and if-else is the way to implement this.

- Add a comment about activation_key being insecure for now. We can fix this once subscription-manager implements <https://issues.redhat.com/browse/ENT-4724> (Eric Gustavsson)

Unittest enhancements for the subscription RegisterCommand change:

- Add global_tool_opts fixture to conftest.py which monkeypatches a fresh ToolOpts into convert2rhel.toolopts.tool_opts. That way tests can modify that without worrying about polluting other tests.
 - How toolopts is imported in the code makes a difference whether this fixture is sufficient or if you need to do a little more work. If the import is::

```
from convert2rhel import toolopts
do_something(toolopts.tool_opts.username)
```

then your test can just do::

```
def test_thing_that_uses_toolopts(global_tool_opts):
    global_tool_opts.username = 'badger'
```

Most of our code, though, imports like this::

```
# In subscription.py, for instance
from convert2rhel.toolopts import tool_opts
do_something(tool_opts.username)
```

so the tests should do something like this::

```
def test_toolopts_differently(global_test_opts, monkeypatch):
    monkeypatch.setattr(subscription, 'tool_opts', global_tool_opts)
```

- Add unittests for utils.run_cmd_in_ptty()
- Add unittests for the subscription.RegistrationCommand object.
- subscription_test.py::test_hide_secrets was expanded to test without equals sign
- Flaky test appeared within systeminfo_test.py::test_generate_rpm_va due to changes to tool_opts in other tests. A temporary fix is added until the whole test class is changed from unittest to pytest

- Fix failing unittests for RegistrationCommand
- Sometimes a process will close stdout before it is done processing. When that happens, we need to wait() for the process to end before closing the pty. If we don't wait, the process will receive a HUP signal which may end it before it is done.
 - But on RHEL7, pexpect.wait() will throw an exception if you wait on an already finished process. So we need to ignore that exception there.
- Add integration test Check for cve fixes, add 'psutil' to install-testing-depends playbook
- Fix Pexpect.spawn truncating lines on RHEL7. Along with a comment on why the change fixes the bug.



Fixes: <https://issues.redhat.com/browse/RHELC-432>

codecov bot commented on May 10 • edited ▾

Codecov Report

Merging [#492](#) ([960490a](#)) into [main](#) ([8658831](#)) will increase coverage by 1.19% .
The diff coverage is 100.00% .

@@	Coverage Diff			@@
##	main	#492	+/-	##
=====				
+ Coverage	82.46%	83.65%	+1.19%	
=====				
Files	16	16		
Lines	2258	2319	+61	
Branches	383	403	+20	
=====				
+ Hits	1862	1940	+78	
+ Misses	331	314	-17	
Partials	65	65		

Impacted Files	Coverage Δ	
convert2rhel/subscription.py	83.80% <100.00%> (+3.27%)	
convert2rhel/utils.py	69.69% <100.00%> (+5.91%)	

[Continue to review full report at Codecov.](#)

Legend - [Click here to learn more](#)

Δ = absolute <relative> (impact), \emptyset = not affected, ? = missing data

Powered by [Codecov](#). Last update [8658831...960490a](#). Read the [comment docs](#).

lgTM-com bot commented on May 10

Contributor

This pull request introduces 3 alerts and fixes 1 when merging [18edac5](#) into [23fe45a](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

abadger commented on May 10

Member

Author

I believe the lgTM errors are false positives but I would appreciate it if someone else would take a look as lgTM is flagging them as security issues (revealing of private data).

 **SpyTec** reviewed on May 10

[View changes](#)

convert2rhel/utils.py

```
238 + class PexpectSizedWindowSpawn(pexpect.spawn):
239 +     # https://github.com/pexpect/pexpect/issues/134
240 +     def setwinsize(self, rows, cols):
241 +         super(PexpectSizedWindowSpawn, self).setwinsize(rows, 120)
```



SpyTec on May 10

Member

We're removing this workaround in [#475](#) for 0.27 and won't fix it for 0.26

SpyTec commented on May 10

Member

@abadger was there any difference between this and the patch?





SpyTec left a comment • edited ▾

Member

The LGTM warnings seem like false positives

convert2rhel/subscription.py **Outdated**

⌵ Show resolved

convert2rhel/unit_tests/subscription_test.py **Outdated**

⌵ Show resolved

abadger commented on May 10

Member

Author

@abadger was there any difference between this and the patch?

There were quite a few conflicts (there have been changes from Rodolfo and Andrew which were merged after the patch was created) which I had to resolve. (I have asked both of them to take a look at this PR specifically to see whether their changes are still intact.)

lgtm-com **bot** commented on May 10

Contributor

This pull request **introduces 3 alerts** and **fixes 1** when merging [12dc446](#) into [23fe45a](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

lgtm-com **bot** commented on May 10

Contributor

This pull request **introduces 3 alerts** and **fixes 1** when merging [c2a1150](#) into [23fe45a](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

lgTM-com bot commented on May 10

Contributor

This pull request introduces 3 alerts and fixes 1 when merging [68e7ad8](#) into [23fe45a](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information



abadger force-pushed the `fix-sub-mgr-cli-call` branch from [68e7ad8](#) to [085fb11](#)

7 months ago

[Compare](#)

lgTM-com bot commented on May 10

Contributor

This pull request introduces 3 alerts and fixes 1 when merging [085fb11](#) into [23fe45a](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

r0x0d commented on May 10

Member

@abadger was there any difference between this and the patch?

There were quite a few conflicts (there have been changes from Rodolfo and Andrew which were merged after the patch was created) which I had to resolve. (I have asked both of them to take a look at this PR specifically to see whether their changes are still intact.)

Looking at the changes right now.

lgTM-com bot commented on May 10

Contributor

This pull request introduces 3 alerts and fixes 1 when merging [b26c1c6](#) into [23fe45a](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

👁️  **SpyTec** requested review from **r0x0d** and **Andrew-ang9** 7 months ago

👁️ **r0x0d** previously approved these changes on May 11

[View changes](#)



r0x0d left a comment

Member

@abadger most of the changes I proposed here are more aesthetic ones, thus, feel free to accept or deny them!

In an overall, from what I remember from my code in `subscription.py`, everything looks fine with the modifications and merges you did, don't think you missed anything!

convert2rhel/subscription.py Outdated

⌵ Show resolved

convert2rhel/subscription.py Outdated

⌵ Show resolved

convert2rhel/subscription.py Outdated

⌵ Show resolved

convert2rhel/subscription.py Outdated

⌵ Show resolved

convert2rhel/subscription.py Outdated

⌵ Show resolved

11 hidden conversations

[Load more...](#)

convert2rhel/utils.py Outdated

⌵ Show resolved

convert2rhel/utils.py Outdated

⌵ Show resolved

plans/tier0.fmf

⌵ Show resolved

plans/tier0.fmf Outdated

⌵ Show resolved

tests/integration/tier0/check-cve-2022-1662/main.fmf

Outdated

Show resolved

r0x0d commented on May 11

Member

Note: it was not an approval, I selected the `comment` option when submitting the review. Don't know what went wrong.

✕  abadger dismissed r0x0d's stale review via `eeeabe1` 7 months ago

lgTM-com  commented on May 11

Contributor

This pull request **introduces 3 alerts** and **fixes 1** when merging [7cbe6a8](#) into [37b3a00](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

lgTM-com  commented on May 11

Contributor



This pull request **introduces 3 alerts** and **fixes 1** when merging [0bf9ebb](#) into [37b3a00](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

  abadger force-pushed the `fix-sub-mgr-cli-call` branch from [0bf9ebb](#) to [5671a94](#) 7 months ago

[Compare](#)

lgTM-com  commented on May 11

Contributor

This pull request **introduces 3 alerts** and **fixes 1** when merging [5671a94](#) into [37b3a00](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information



fixed alerts:

- 1 for Clear-text logging of sensitive information

 **bocekm** previously approved these changes on May 11

[View changes](#)

✕  **abadger** dismissed **bocekm**'s stale review via `e84faff` 7 months ago

  **abadger** force-pushed the `fix-sub-mgr-cli-call` branch from `5671a94` to `e84faff` 7 months ago

[Compare](#)

abadger commented on May 12

Member

Author

Rebased to pick up the fixes for ubi8

  **abadger** mentioned this pull request on May 12

[RHELC-570] Cleanup pexpect terminal size #475

 Merged

lgTM-com bot commented on May 12

Contributor

This pull request introduces 3 alerts and fixes 1 when merging `e84faff` into `68bf0ac` - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

lgTM-com bot commented on May 12

Contributor

This pull request introduces 3 alerts and fixes 1 when merging `29ab9b8` into `68bf0ac` - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

12 hidden items

[Load more...](#)

lgTM-com bot commented on May 16

Contributor

This pull request **introduces 3 alerts** and **fixes 1** when merging [36e0e98](#) into [a921086](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information



danmyway force-pushed the `fix-sub-mgr-cli-call` branch from [36e0e98](#) to [e9816db](#)

6 months ago

[Compare](#)

lgTM-com bot commented on May 16

Contributor

This pull request **introduces 3 alerts** and **fixes 1** when merging [e9816db](#) into [a921086](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

lgTM-com bot commented on May 16

Contributor

This pull request **introduces 3 alerts** and **fixes 1** when merging [34fcd31](#) into [a921086](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information



fixed alerts:

- 1 for Clear-text logging of sensitive information

danmyway commented on May 26

Member

All tests have passed, @bocekm

  danmyway added the `need-final-approval` label on May 26

 bocekm previously approved these changes on May 26

[View changes](#)

r0x0d commented on May 26

















Member







@abadger +1 for that toolopts fixture.

 r0x0d previously approved these changes on May 26



[View changes](#)

 abadger and others added 11 commits 6 months ago

- | | |
|--|----------|
|   Do not put the subscription-manager password onto the command line. ... | b312278 |
|   Fix missing colon in testing farm metadata | e2d8992 |
|   Ignore false positives from lgtm ... | 09ec252 |
|   Update subscription-manager interaction to expect password or Password ... | a7ac432 |
|   Rename cve integration test. ... | 0220f84 |
|   Apply changes from Rodolfo's code review. | 2382f1d |
|   Add docstrings ... | 77a04f6 |
|   Fix sample password used in the integration test to not trigger gitle... ... | facbbcfc |

-   Edit testing dependencies playbook ... 564ec4e
-   Add comment about why FakeSpawn in unittests is not global ... df1b793
-   Implement .gitleaks.toml to ignore gitleaks false positive. ... ✗ 960490a

  **abadger** dismissed stale reviews from **r0x0d** and **bocekm** via 960490a 6 months ago

  **abadger** force-pushed the `fix-sub-mgr-cli-call` branch from **34fcd31** to **960490a** 6 months ago

[Compare](#)

r0x0d approved these changes on May 26

[View changes](#)

lgtn-com bot commented on May 26

Contributor


This pull request **introduces 3 alerts** and **fixes 1** when merging [960490a](#) into [8658831](#) - [view on LGTM.com](#)

new alerts:

- 3 for Clear-text logging of sensitive information

fixed alerts:

- 1 for Clear-text logging of sensitive information

 **bocekm** merged commit **8d72fb0** into [oamg:main](#) on May 27
16 of 17 checks passed

[View details](#)

 **r0x0d** pushed a commit to `r0x0d/convert2rhel` that referenced this pull request on Jun 1

 Do not put the subscription-manager password onto the command line. ([o...](#) ... [00e1f6f](#)

  **SpyTec** mentioned this pull request on Jun 3

Bump version to 0.26 #506

 **Merged**

 **Andrew-ang9** pushed a commit to `Andrew-ang9/convert2rhel` that referenced this pull request on Jun 16





Do not put the subscription-manager password onto the command line. ([o...](#) ...)

d698b01



abadger deleted the `fix-sub-mgr-cli-call` branch 4 months ago

Reviewers



SpyTec



r0x0d



bocekmm



Andrew-ang9



Assignees

No one assigned

Labels

need-final-approval

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

5 participants

