# Pulp - Issue #3521

## last_override_config exposes sensitive info

03/23/2018 02:30 AM - rmcgover

| | | | |
|---|---|---|---|
| **Status:** | CLOSED - CURRENTRELEASE | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | bmbouter | **Estimated time:** | 0:00 hour |
| **Category:** | | | |
| **Sprint/Milestone:** | | | |
| **Severity:** | 2. Medium | **Groomed:** | Yes |
| **Version:** | | **Sprint Candidate:** | No |
| **Platform Release:** | 2.16.2 | **Tags:** | Pulp 2 |
| **OS:** | | **Sprint:** | Sprint 38 |
| **Triaged:** | Yes | **Quarter:** | |

**Description**

Importers and distributors have a "last_override_config" object which is exposed via the API.

In several cases, secrets are passed into override_config when triggering a task. For example, in yum importer there's ssl_client_key and in docker importer there's basic_auth_password. If these config items are given, they're stored in last_override_config and then become readable to all users with read access on the distributor/importer.

This makes usage of those config items quite dangerous as one can't pass these secrets into the API for a sync without also considering which users have read access on the objects, and whether it's OK to expose the secret to those users. Or more likely, one would fail to consider this, and thus would build tools/workflows which expose the secrets without realizing it.

That latter scenario is exactly what I'm faced with now, because it has always been established procedure that our Pulp installations internally have widely shared read-only accounts, allowing everyone to freely data mine / build applications on top of our Pulp without administrative hassle. Due to realization of this issue, that's now under threat and we may be forced to make the system less convenient.

Solution:
- Keep the secrets in the DB but don't render them in the API

**Related issues:**

| | |
|---|---|
| Related to Pulp - Issue #4083: Non-sensitive information is not being display... | **CLOSED - WONTFIX** |

### Associated revisions

**Revision 9c776506 - 06/01/2018 10:50 PM - bmbouter**

Redact last_override_config

This commit resolvs CVE-2018-1090 by redacting all data from last_override_config. It does not modify what is saved in the database. It also adds a release note for the 2.16.2 release.

https://pulp.plan.io/issues/3521 closes #3521

**Revision 723672e3 - 06/18/2018 08:09 PM - bmbouter**

Redact last_override_config

This commit resolvs CVE-2018-1090 by redacting all data from last_override_config. It does not modify what is saved in the database. It also adds a release note for the 2.16.2 release.

https://pulp.plan.io/issues/3521 closes #3521

(cherry picked from commit 9c776506a1fdbd70fc95547516288f549b80ccbf)

## History

#### #2 - 03/23/2018 04:02 PM - bmbouter

+1 to keeping the options in the db and not rendering them in the API. What if we add a new option that allows the sensitive keys to be listed by the user. Then the API just hides those.

#### #3 - 03/23/2018 09:10 PM - kseifried@redhat.com

This has been assigned CVE-2018-1090, can we make this public? Thanks.

#### #4 - 03/23/2018 09:41 PM - bmbouter

*- Private changed from Yes to No*

I'm +1 on making it public as were all other devs in chat earlier. I'm making that change now per @kurt's recommendation.

Also it would be great if we could get a fix contributed that allows the user to hide the credentials that are displayed.

#### #6 - 03/27/2018 04:41 PM - dalley

*- Triaged changed from No to Yes*

*- Sprint Candidate changed from No to Yes*

#### #9 - 05/14/2018 05:48 PM - ttereshc

+1 for - Keep the secrets in the DB but don't render them in the API

#### #10 - 05/25/2018 02:03 PM - ttereshc

*- Description updated*

*- Groomed changed from No to Yes*

#### #11 - 06/01/2018 03:24 PM - rchan

*- Sprint set to Sprint 38*

#### #12 - 06/01/2018 04:10 PM - rchan

*- Sprint Candidate changed from Yes to No*

#### #13 - 06/01/2018 08:28 PM - bmbouter

*- Status changed from NEW to ASSIGNED*

*- Assignee set to bmbouter*

#### #14 - 06/01/2018 10:48 PM - bmbouter

*- Status changed from ASSIGNED to POST*

PR available at: https://github.com/pulp/pulp/pull/3513

#### #15 - 06/01/2018 10:54 PM - bmbouter

I could reproduce easily by starting with the default zoo repo from pulp-admin. Then I caused a sync with an override specified:

```
curl --insecure -X POST --user admin:admin -d '{"override_config": {"feed": "https://example.com"}}' https://l
ocalhost/pulp/api/v2/repositories/zoo/actions/sync/
```

Then without the patch applied I show the serialized importer which shows the data in last_override_config:

```
curl --insecure -X GET --user admin:admin https://localhost/pulp/api/v2/repositories/zoo/importers/yum_importe
r/ | jq
{
  "repo_id": "zoo",
  "last_updated": "2018-06-01T18:44:02Z",
  "_href": "/pulp/api/v2/repositories/zoo/importers/yum_importer/",
  "_ns": "repo_importers",
  "importer_type_id": "yum_importer",
  "last_override_config": {
    "feed": "https://example.com"
  },
  "last_sync": "2018-06-01T20:10:02Z",
  "scratchpad": {
    "repomd_revision": 1331832478
  },
  "_id": {
    "$oid": "5b1193f230f252206fea660d"
  },
  "config": {
    "feed": "https://repos.fedorapeople.org/repos/pulp/pulp/demo_repos/zoo/"
  },
  "id": "yum_importer"
}
```

Then applying the patch the output now looks like:

```
curl --insecure -X GET --user admin:admin https://localhost/pulp/api/v2/repositories/zoo/importers/yum_importe
r/ | jq
{
  "repo_id": "zoo",
  "last_updated": "2018-06-01T18:44:02Z",
  "_href": "/pulp/api/v2/repositories/zoo/importers/yum_importer/",
  "_ns": "repo_importers",
  "importer_type_id": "yum_importer",
  "last_override_config": {},
  "last_sync": "2018-06-01T20:10:02Z",
  "scratchpad": {
    "repomd_revision": 1331832478
  },
  "_id": {
    "$oid": "5b1193f230f252206fea660d"
  },
  "config": {
    "feed": "https://repos.fedorapeople.org/repos/pulp/pulp/demo_repos/zoo/"
  },
  "id": "yum_importer"
}
```

#### #16 - 06/04/2018 05:21 PM - bmbouter

*- Status changed from POST to MODIFIED*

Applied in changeset pulp|9c776506a1fdbd70fc95547516288f549b80ccbf.

#### #18 - 06/15/2018 01:53 PM - dkliban@redhat.com

*- Platform Release set to 2.16.2*

#### #19 - 06/18/2018 08:09 PM - bmbouter

Applied in changeset pulp|723672e315bbdd096801943c2c787fcf889b7523.

#### #20 - 06/25/2018 07:19 PM - lchimonji10

See: https://github.com/PulpQE/pulp-smash/pull/1088

#### #21 - 09/12/2018 06:32 PM - bmbouter

*- Status changed from MODIFIED to CLOSED - CURRENTRELEASE*

I'm not sure why this is not at MODIFIED, but from the associated commits (links also below), I can see the code lives on the 2.16-release, 2.17-release, and 2-master so I'm moving to CLOSED - CURRENTRELEASE.

https://github.com/pulp/pulp/commit/9c776506a1fdbd70fc95547516288f549b80ccbf
https://github.com/pulp/pulp/commit/723672e315bbdd096801943c2c787fcf889b7523

#### #22 - 10/12/2018 05:31 PM - daviddavis

*- Related to Issue #4083: Non-sensitive information is not being displayed for last_override_config added*

#### #23 - 04/15/2019 10:12 PM - bmbouter

*- Tags Pulp 2 added*